FUJITSU

FUJITSU Server PRIMERGY RX2520 M1

Upgrade and Maintenance Manual

Edition February 2014

Comments… Suggestions… Corrections…

The User Documentation Department would like to know your opinion of this manual. Your feedback helps us optimize our documentation to suit your individual needs.

Feel free to send us your comments by e-mail to manuals@ts.fujitsu.com.

Certified documentation according to DIN EN ISO 9001:2008

To ensure a consistently high quality standard and user-friendliness, this documentation was created to meet the regulations of a quality management system which complies with the requirements of the standard DIN EN ISO 9001:2008.

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

Copyright and Trademarks

Copyright © 2014 Fujitsu Technology Solutions GmbH.

All rights reserved.
Delivery subject to availability; right of technical modifications reserved.

All hardware and software names used are trademarks of their respective manufacturers.

– The contents of this manual may be revised without prior notice.
– Fujitsu assumes no liability for damages to third party copyrights or other rights arising from the use of any information in this manual.
– No part of this manual may be reproduced in any form without the prior written permission of Fujitsu.

Microsoft, Windows, Windows Server, and Hyper V are trademarks or registered trademarks of Microsoft Corporation in the USA and other countries.

Intel and Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the USA and other countries.

Before reading this manual

For your safety

This manual contains important information for safely and correctly using this product.

Carefully read the manual before using this product. Pay particular attention to the accompanying manual "Safety Notes and Regulations" and ensure these safety notes are understood before using the product. Keep this manual and the manual "Safety Notes and Regulations" in a safe place for easy reference while using this product.

Radio interference

This product is a "Class A" ITE (Information Technology Equipment). In a domestic environment this product may cause radio interference, in which case the user may be required to take appropriate measures. VCCI-A

Aluminum electrolytic capacitors

The aluminum electrolytic capacitors used in the product's printed circuit board assemblies and in the mouse and keyboard are limited-life components. Use of these components beyond their operating life may result in electrolyte leakage or depletion, potentially causing emission of foul odor or smoke.

As a guideline, in a normal office environment (25°C) operating life is not expected to be reached within the maintenance support period (5 years). However, operating life may be reached more quickly if, for example, the product is used in a hot environment. The customer shall bear the cost of replacing replaceable components which have exceeded their operating life. Note that these are only guidelines, and do not constitute a guarantee of trouble-free operation during the maintenance support period.

High safety use

This product has been designed and manufactured to be used in commercial and/or industrial areas as a server.

When used as visual display workplace, it must not be placed in the direct field of view to avoid incommoding reflections (applies only to TX server systems).

The device has not been designed or manufactured for uses which demand an extremely high level of safety and carry a direct and serious risk of life or body if such safety cannot be assured.

These uses include control of nuclear reactions in nuclear power plants, automatic airplane flight control, air traffic control, traffic control in mass transport systems, medical devices for life support, and missile guidance control in weapons systems (hereafter, "high safety use"). Customers should not use this product for high safety use unless measures are in place for ensuring the level of safety demanded of such use. Please consult the sales staff of Fujitsu if intending to use this product for high safety use.

Measures against momentary voltage drop

This product may be affected by a momentary voltage drop in the power supply caused by lightning. To prevent a momentary voltage drop, use of an AC uninterruptible power supply is recommended.

(This notice follows the guidelines of Voltage Dip Immunity of Personal Computer issued by JEITA, the Japan Electronics and Information Technology Industries Association.)

Technology controlled by the Foreign Exchange and Foreign Trade Control Law of Japan

Documents produced by Fujitsu may contain technology controlled by the Foreign Exchange and Foreign Trade Control Law of Japan. Documents which contain such technology should not be exported from Japan or transferred to non-residents of Japan without first obtaining authorization in accordance with the above law.

Harmonic Current Standards

This product conforms to harmonic current standard JIS C 61000-3-2.

Only for the Japanese market: About SATA hard disk drives

The SATA version of this server supports hard disk drives with SATA / BC-SATA storage interfaces. Please note that the usage and operation conditions differ depending on the type of hard disk drive used.

Please refer to the following internet address for further information on the usage and operation conditions of each available type of hard disk drive:

(*http://jp.fujitsu.com/platform/server/primergy/manual/*)

Only for the Japanese market:

Although described in this manual, some sections do not apply to the Japanese market. These options and routines include:

– CSS (Customer Self Service)

Version history

Issue number	Reason for update
Review	Review
February 2014	Initial release

Contents

1 Introduction 21

1.1 Notational conventions 22

2 Before you start 23

2.1 Classification of procedures 25
2.1.1 Customer Replaceable Units (CRU) 25
2.1.2 Upgrade and Repair Units (URU) 26
2.1.3 Field Replaceable Units (FRU) 27

2.2 Average task duration 27

2.3 Tools you need at hand 28

2.4 Documents you need at hand 31

3 Important information 35

3.1 Safety instructions 35

3.2 ENERGY STAR 43

3.3 CE conformity 43

3.4 FCC Class A Compliance Statement 44

3.5 Environmental protection 45

4 Basic hardware procedures 47

4.1 Using diagnostics information 47
4.1.1 Locating the defective server 47
4.1.2 Determining the error class 48
4.1.2.1 Global Error indicator 48
4.1.2.2 Customer Self Service (CSS) indicator 48
4.1.3 Locating the defective component 49
4.1.3.1 Local diagnostic indicators on the front 49

4.2 Shutting down the server 49

4.3 Disconnecting power cords 50

4.4 Getting access to the component 51
4.4.1 Extending the server out of the rack 51
4.4.2 Removing the server from the rack 53
4.4.3 Opening the server 54
4.4.3.1 Removing the housing cover 55
4.4.3.2 Removing the air duct 56

4.5 Reassembling 57
4.5.1 Installing the air duct 57
4.5.2 Closing the server 58
4.5.2.1 Mounting the housing cover 59
4.5.3 Mounting the server in the rack 59
4.5.3.1 Seating the server on the rack rails 59
4.5.3.2 Sliding the server into the rack 62

4.6 Connecting the server to the power source 62

4.7 Switching on the server 64

5 Basic software procedures 65

5.1 Starting the maintenance task 65
5.1.1 Disabling BitLocker functionality 65
5.1.2 Disabling SVOM boot watchdog functionality 66
5.1.2.1 Viewing boot watchdog settings 66
5.1.2.2 Configuring boot watchdog settings 67
5.1.3 Removing backup and optical disk media 69
5.1.4 Verifying and configuring the backup software solution 69
5.1.5 Note on server maintenance in a Multipath I/O environment . . . 70
5.1.6 Switching on the ID indicator 72

5.2 Completing the maintenance task 73
5.2.1 Updating or recovering the system board BIOS and iRMC 73
5.2.1.1 Updating or recovering the system board BIOS 73
5.2.1.2 Updating or recovering the iRMC 74
5.2.2 Verifying system information backup / restore 75
5.2.3 Updating RAID controller firmware 77
5.2.4 Enabling Option ROM scan 78
5.2.5 Verifying and configuring the backup software solution 79
5.2.6 Resetting the boot retry counter 80
5.2.6.1 Viewing the boot retry counter 80
5.2.6.2 Resetting the boot retry counter 80

5.2.7 Enabling SVOM boot watchdog functionality 82
5.2.8 Enabling replaced components in the system BIOS 82
5.2.9 Verifying the memory mode 83
5.2.10 Verifying the system time settings 84
5.2.11 Viewing and clearing the System Event Log (SEL) 85
5.2.11.1 Viewing the SEL 85
5.2.11.2 Clearing the SEL 86
5.2.12 Updating the NIC configuration file in a Linux environment . . . 86
5.2.13 Enabling BitLocker functionality 88
5.2.14 Performing a RAID array rebuild 89
5.2.15 Looking up changed MAC / WWN addresses 89
5.2.15.1 Looking up MAC addresses 89
5.2.15.2 Looking up WWN addresses 90
5.2.16 Using the Chassis ID Prom Tool 91
5.2.17 Configuring LAN teaming 92
5.2.17.1 After replacing / upgrading LAN controllers 92
5.2.17.2 After replacing the system board 92
5.2.18 Switching off the ID indicator 93
5.2.19 Performing a fan test after replacing a defective fan 93

6 Power supply units 95

6.1 Basic information 95
6.1.1 Power supply unit configurations 96
6.1.2 Assembly rules 96
6.1.3 Power supply unit slots 97

6.2 Installing hot-plug power supply units 97
6.2.1 Preliminary steps 97
6.2.2 Removing the dummy cover 98
6.2.3 Installing a hot-plug power supply unit 99
6.2.4 Concluding steps 99

6.3 Removing a hot-plug power supply unit 100
6.3.1 Preliminary steps 100
6.3.2 Removing a hot-plug power supply unit 101
6.3.3 Installing a dummy cover 102
6.3.4 Concluding steps 102

6.4 Replacing a hot-plug power supply unit 103
6.4.1 Preliminary steps 103
6.4.2 Removing the defective hot-plug power supply unit 103
6.4.3 Installing the new hot-plug power supply unit 104

6.4.4 Concluding steps 104

6.5 Upgrading a power supply from 450 W to 800 W 105
6.5.1 Preliminary steps 105
6.5.2 Removing the hot-plug power supply unit 105
6.5.3 Installing the new hot-plug power supply unit 106
6.5.4 Concluding steps 107

6.6 Replacing the power backplane 107
6.6.1 Preliminary steps 107
6.6.2 Disconnecting cables 108
6.6.3 Removing the power backplane 108
6.6.4 Installing the power backplane 110
6.6.5 Reconnecting cables 112
6.6.6 Concluding steps 113

7 Hard disk drives / solid state drives 115

7.1 Basic procedures 116

7.2 2.5-inch HDD / SSD configurations 116
7.2.1 Mounting order for 2.5-inch HDDs / SSDs 116
7.2.1.1 HDD / SSD mounting order for 4x 2.5-inch HDD / SSD configuration 117
7.2.1.2 HDD / SSD naming scheme for 4x 2.5-inch HDD / SSD configuration 117
7.2.1.3 HDD / SSD mounting order for 8x 2.5-inch HDD / SSD configurations 118
7.2.1.4 HDD / SSD naming scheme for 8x 2.5-inch HDD / SSD configurations 119
7.2.1.5 HDD / SSD mounting order for 12x 2.5-inch HDD / SSD configuration 119
7.2.1.6 HDD / SSD naming scheme for 12x 2.5-inch HDD / SSD configuration 119
7.2.1.7 HDD / SSD mounting order for 16x 2.5-inch HDD / SSD configuration 120
7.2.1.8 HDD / SSD naming scheme 16x 2.5-inch HDD / SSD configuration 121
7.2.2 Installing 2.5-inch HDD / SSD modules 121
7.2.2.1 Preliminary steps 122
7.2.2.2 Removing a 2.5-inch dummy module 122
7.2.2.3 Installing a 2.5-inch HDD / SSD module 123
7.2.2.4 Concluding steps 124

7.2.3 Removing 2.5-inch HDD / SSD modules 124
7.2.3.1 Preliminary steps 124
7.2.3.2 Removing a 2.5-inch HDD / SSD module 125
7.2.3.3 Installing a 2.5-inch dummy module 126
7.2.3.4 Concluding steps 127
7.2.4 Replacing a 2.5-inch HDD / SSD module 127
7.2.4.1 Preliminary steps 128
7.2.4.2 Removing a 2.5-inch HDD / SSD module 128
7.2.4.3 Installing a 2.5-inch HDD / SSD module 128
7.2.4.4 Concluding steps 128

7.3 Replacing SAS / SATA HDD / SSD backplanes 129
7.3.1 Replacing the 4x 2.5-inch HDD SAS backplane 129
7.3.1.1 Preliminary steps 129
7.3.1.2 Removing the 4x 2.5-inch SAS HDD backplane 130
7.3.1.3 Installing the 4x 2.5-inch HDD SAS backplane 131
7.3.1.4 Concluding steps 132
7.3.2 Replacing the 12x 2.5-inch HDD SAS backplane 132
7.3.2.1 Preliminary steps 132
7.3.2.2 Removing the 12x2.5-inch HDD SAS backplane 133
7.3.2.3 Installing the 12x 2.5-inch HDD SAS backplane 135
7.3.2.4 Concluding steps 137

7.4 HDD cage 137
7.4.1 Removing a HDD cage 137
7.4.2 Installing a HDD cage 139

8 System fan 141

8.1 Basic information 141

8.2 Replacing the system fan 142
8.2.1 Preliminary steps 142
8.2.2 Removing a system fan 142
8.2.3 Installing a system fan 143
8.2.4 Concluding steps 143

8.3 Removing the fan box 144
8.3.1 Preliminary steps 144
8.3.2 Removing the fan box 144
8.3.3 Installing the fan box 146
8.3.4 Concluding steps 147

9 Expansion cards and backup units 149

9.1 Basic information 149

9.2 Handling slot brackets 153
9.2.1 Installing a slot bracket 153
9.2.1.1 Installing a standard slot bracket 153
9.2.1.2 Installing a slot bracket to the Network adapter D2755 . . . 155
9.2.1.3 Installing a slot bracket to the USB 3.0 interface card D3305 . . 157
9.2.2 Removing a slot bracket 158

9.3 Expansion cards 159
9.3.1 Installing expansion cards 159
9.3.1.1 Preliminary steps 159
9.3.1.2 Removing the slot bracket 160
9.3.1.3 Installing an expansion card 160
9.3.1.4 Concluding steps 161
9.3.2 Removing expansion cards 162
9.3.2.1 Preliminary steps 162
9.3.2.2 Removing an expansion card 162
9.3.2.3 Installing a PCI slot bracket 164
9.3.2.4 Concluding steps 164
9.3.3 Replacing expansion cards 165
9.3.3.1 Preliminary steps 165
9.3.3.2 Removing an expansion card 165
9.3.3.3 Installing an expansion card 166
9.3.3.4 Connecting cables to the expansion card 166
9.3.3.5 Connecting a battery backup unit to the expansion card . . 166
9.3.3.6 Concluding steps 166

9.4 SAS RAID controller in PCI slot 7 167
9.4.1 Installing the SAS RAID controller 167
9.4.1.1 Preliminary steps 167
9.4.1.2 Preparing the SAS RAID controller 167
9.4.1.3 Installing the SAS RAID controller 168
9.4.1.4 Connecting cables to the expansion card 169
9.4.1.5 Connecting a backup unit to the expansion card 169
9.4.1.6 Concluding steps 169
9.4.2 Removing the SAS RAID controller 170
9.4.2.1 Preliminary steps 170
9.4.2.2 Removing the SAS RAID controller 170
9.4.2.3 Removing the SAS RAID card holder 171

9.4.2.4 Concluding steps . . . 171
9.4.3 Replacing the SAS RAID controller . . . 172
9.4.3.1 Preliminary steps . . . 172
9.4.3.2 Removing the defective SAS RAID controller . . . 172
9.4.3.3 Installing the new SAS RAID controller . . . 172
9.4.3.4 Connecting cables to the expansion card . . . 172
9.4.3.5 Connecting a backup unit to the expansion card . . . 173
9.4.3.6 Concluding steps . . . 173

9.5 Backup Units . . . 174
9.5.1 Basic information . . . 174
9.5.2 Installing a FBU . . . 174
9.5.2.1 Preliminary steps . . . 175
9.5.2.2 Installing TFM to the RAID controller (if applicable) . . . 175
9.5.2.3 Preparing the FBU . . . 176
9.5.2.4 Connecting the FBU cable to the FBU . . . 177
9.5.2.5 Installing the FBU holder onto the air duct . . . 178
9.5.2.6 Installing the air duct with an FBU . . . 180
9.5.2.7 Concluding steps . . . 180
9.5.3 Removing a FBU . . . 181
9.5.3.1 Preliminary steps . . . 181
9.5.3.2 Removing the air duct with an FBU . . . 182
9.5.3.3 Removing the FBU holder from the air duct . . . 182
9.5.3.4 Concluding steps . . . 183
9.5.4 Replacing a FBU . . . 183
9.5.4.1 Preliminary steps . . . 183
9.5.4.2 Removing a FBU from the air duct . . . 184
9.5.4.3 Disconnecting the FBU cable from the FBU . . . 184
9.5.4.4 Removing the FBU from the holder . . . 185
9.5.4.5 Installing a new FBU . . . 185
9.5.4.6 Concluding steps . . . 185

9.6 Handling SFP+ transceiver modules . . . 186
9.6.1 Installing SFP+ transceiver modules . . . 186
9.6.2 Removing an SFP+ transceiver module . . . 190
9.6.3 Replacing SFP+ transceiver modules . . . 193

10 Main memory . . . 195

10.1 Basic information . . . 196
10.1.1 Memory sequence . . . 197
10.1.1.1 Population rules . . . 197

10.1.1.2 Independant Channel mode . . . 198
10.1.1.3 Performance modes . . . 198

10.2 Installing memory modules . . . 199
10.2.1 Preliminary steps . . . 199
10.2.2 Installing a memory module . . . 199
10.2.3 Concluding steps . . . 200

10.3 Removing memory modules . . . 201
10.3.1 Preliminary steps . . . 201
10.3.2 Removing a memory module . . . 201
10.3.3 Concluding steps . . . 202

10.4 Replacing memory modules . . . 202
10.4.1 Preliminary steps . . . 202
10.4.2 Removing the defective memory module . . . 203
10.4.3 Installing a new memory module . . . 203
10.4.4 Concluding steps . . . 203

11 Processors . . . 205

11.1 Basic information . . . 206
11.1.1 Supported processors . . . 206
11.1.2 Processor locations . . . 206

11.2 Installing processors . . . 207
11.2.1 Preliminary steps . . . 207
11.2.2 Installing the processor . . . 207
11.2.2.1 Removing the protective cover . . . 208
11.2.2.2 Installing the new processor . . . 209
11.2.3 Concluding steps . . . 211

11.3 Removing processors . . . 212
11.3.1 Preliminary steps . . . 212
11.3.2 Removing a processor . . . 212
11.3.2.1 Installing the protective cover . . . 215
11.3.3 Concluding steps . . . 216

11.4 Upgrading or replacing processors . . . 216
11.4.1 Preliminary steps . . . 217
11.4.2 Upgrading or replacing a processor . . . 217
11.4.3 Concluding steps . . . 217

11.5 Handling processor heat sinks . . . 219
11.5.1 Preliminary steps . . . 219

11.5.2 Installing processor heat sinks . . . 219
11.5.2.1 Preparing the heat sink and processor . . . 220
11.5.2.2 Installing the heat sink . . . 221
11.5.3 Removing processor heat sinks . . . 222
11.5.4 Replacing processor heat sinks . . . 223
11.5.4.1 Removing the processor heat sink . . . 223
11.5.4.2 Applying thermal paste . . . 224
11.5.4.3 Installing the processor heat sink . . . 224
11.5.5 Concluding steps . . . 224

11.6 Applying thermal paste . . . 225

12 Accessible drives . . . 227

12.1 Basic informations . . . 228

12.2 Installing a Local Service Display (LSD) module . . . 229
12.2.1 Preliminary steps . . . 229
12.2.2 Removing the LSD dummy cover . . . 230
12.2.3 Installing a LSD module . . . 231
12.2.4 Concluding steps . . . 232

12.3 Removing a LSD module . . . 232
12.3.1 Preliminary steps . . . 232
12.3.2 Removing the LSD module . . . 233
12.3.3 Concluding steps . . . 235

12.4 Replacing a LSD module . . . 235
12.4.1 Preliminary steps . . . 236
12.4.2 Removing the defective LSD module . . . 236
12.4.3 Installing the new LSD module . . . 236
12.4.4 Concluding steps . . . 236

12.5 Installing the optical disk drive (ODD) . . . 236
12.5.1 Preliminary steps . . . 237
12.5.2 Removing the ODD dummy module . . . 237
12.5.3 Preparing an ODD . . . 238
12.5.4 Installing an ODD . . . 240
12.5.5 Concluding steps . . . 241

12.6 Removing the optical disc drive (ODD) . . . 242
12.6.1 Preliminary steps . . . 242
12.6.2 Removing the ODD . . . 242
12.6.3 Concluding steps . . . 244

12.7 Replacing an ODD 244
12.7.1 Preliminary steps 245
12.7.2 Removing the defective ODD 245
12.7.3 Installing the new ODD 245
12.7.4 Concluding steps 245

12.8 Installing a RDX drive in 2.5-inch version 246
12.8.1 Preliminary steps 246
12.8.2 Installing a RDX drive in the cage 246
12.8.3 Installing the RDX drive 248
12.8.4 Connecting the RDX drive 249
12.8.4.1 Connecting the RDX drive to the system board 249
12.8.4.2 Connecting the RDX drive to the USB 3.0 interface card . . 249
12.8.5 Concluding steps 251

12.9 Removing a RDX drive in 2.5-inch version 251
12.9.1 Preliminary steps 251
12.9.2 Removing the drive cage 251
12.9.3 Removing a RDX drive out of the cage 253
12.9.4 Concluding steps 255

12.10 Replacing the RDX drive in 2.5-inch version 255
12.10.1 Preliminary steps 255
12.10.2 Removing the defective RDX drive 256
12.10.3 Installing the new RDX drive 256
12.10.4 Concluding steps 256

12.11 Installing an LTO drive in 2.5-inch version 256
12.11.1 Preliminary steps 257
12.11.2 Removing the drive cage 257
12.11.3 Removing the tape drive dummy module 258
12.11.4 Installing an LTO drive in the cage 259
12.11.5 Installing the LTO cage 261
12.11.6 Concluding steps 262

12.12 Removing an LTO drive in 2.5-inch version 263
12.12.1 Preliminary steps 263
12.12.2 Removing the drive cage 264
12.12.3 Removing an LTO drive out of the cage 265
12.12.4 Installing the tape drive dummy module 267
12.12.5 Concluding steps 269

12.13 Replacing the LTO drive in 2.5-inch version 270
12.13.1 Preliminary steps 270
12.13.2 Removing the defective LTO drive 270

12.13.3 Installing the new LTO drive 270
12.13.4 Concluding steps 270

13 Front panel and external connectors 273

13.1 Front panel module 273
13.1.1 Replacing the front panel module 273
13.1.1.1 Preliminary steps 274
13.1.1.2 Removing the front panel module 275
13.1.1.3 Installing the front panel module 275
13.1.1.4 Concluding steps 277

13.2 Front VGA connector 278
13.2.1 Installing the front VGA connector 278
13.2.1.1 Preliminary steps 278
13.2.1.2 Removing the front panel module 278
13.2.1.3 Preparing the front panel module 279
13.2.1.4 Installing the front VGA connector 279
13.2.1.5 Re-installing the front panel module 280
13.2.1.6 Concluding steps 281
13.2.2 Removing the front VGA connector 282
13.2.2.1 Preliminary steps 282
13.2.2.2 Removing the front VGA cable 282
13.2.2.3 Removing the front VGA connector 283
13.2.2.4 Re-installing the front panel module 283
13.2.2.5 Concluding steps 283
13.2.3 Replacing the front VGA connector 284
13.2.3.1 Preliminary steps 284
13.2.3.2 Removing the front panel module 284
13.2.3.3 Removing the front VGA connector 284
13.2.3.4 Installing the new front VGA connector 284
13.2.3.5 Re-installing the front panel module 284
13.2.3.6 Concluding steps 284

13.3 Front cage 285
13.3.1 Replacing the front panel cage 285
13.3.1.1 Preliminary steps 285
13.3.1.2 Removing the front panel cage 285
13.3.1.3 Re-installing the front panel cage 287
13.3.1.4 Concluding steps 289

14 System board and components 291

14.1 Basic information 291

14.2 Replacing the CMOS battery 292
14.2.1 Preliminary steps 292
14.2.2 Removing the battery 293
14.2.3 Installing the CMOS battery 294
14.2.4 Concluding steps 294

14.3 USB Flash Module (UFM) 295
14.3.1 Installing the UFM 295
14.3.1.1 Preliminary steps 295
14.3.1.2 Installing the UFM 296
14.3.1.3 Concluding steps 297
14.3.1.4 Software configuration 297
14.3.2 Removing the UFM 298
14.3.2.1 Preliminary steps 298
14.3.2.2 Removing the UFM 299
14.3.2.3 Concluding steps 299
14.3.3 Replacing the UFM 299
14.3.3.1 Preliminary steps 300
14.3.3.2 Removing the UFM 300
14.3.3.3 Installing the new UFM 300
14.3.3.4 Concluding steps 303
14.3.3.5 Software configuration 303

14.4 Trusted Platform Module (TPM) 304
14.4.1 Installing the TPM 304
14.4.1.1 Preliminary steps 304
14.4.1.2 Installing the TPM 305
14.4.1.3 Concluding steps 307
14.4.2 Removing the TPM 309
14.4.2.1 Preliminary steps 310
14.4.2.2 Removing the TPM 311
14.4.2.3 Concluding steps 313
14.4.3 Replacing the TPM 313
14.4.3.1 Preliminary steps 313
14.4.3.2 Removing the TPM 314
14.4.3.3 Re-installing the TPM 314
14.4.3.4 Concluding steps 315

14.5 Onboard SAS enabling key 315
14.5.1 Installing the onboard SAS enabling key 315

14.5.1.1 Preliminary steps . . . 315
14.5.1.2 Installing the onboard SAS enabling key . . . 316
14.5.1.3 Concluding steps . . . 317
14.5.2 Removing the onboard SAS enabling key . . . 317
14.5.2.1 Preliminary steps . . . 317
14.5.2.2 Removing onboard SAS enabling key . . . 318
14.5.2.3 Concluding steps . . . 318
14.5.3 Replacing the onboard SAS enabling key . . . 318
14.5.3.1 Preliminary steps . . . 319
14.5.3.2 Replacing the onboard SAS enabling key . . . 319
14.5.3.3 Concluding steps . . . 319

14.6 Replacing the system board . . . 319
14.6.1 Preliminary steps . . . 322
14.6.2 Removing the defective system board . . . 323
14.6.3 Installing the system board . . . 326
14.6.3.1 Mounting the system board . . . 326
14.6.3.2 Swapping processors . . . 327
14.6.4 Concluding steps . . . 328

15 Cables . . . 331

15.1 List of used cables . . . 331

15.2 Cabling plans . . . 334
15.2.1 Configuration 2 . . . 334
15.2.2 Configuration 3 . . . 336
15.2.3 Configuration 4 . . . 337
15.2.4 Configuration 5 . . . 338
15.2.5 Configuration 6 . . . 340
15.2.6 Configuration 7 . . . 341
15.2.7 Configuration 8 . . . 342

16 Appendix . . . 343

16.1 Mechanical overview . . . 343
16.1.1 Server front . . . 343
16.1.2 Server rear . . . 344
16.1.3 Server interior . . . 345

16.2 Configuration tables . . . 346
16.2.1 Hard disk drives / solid state drives mounting order . . . 346

16.2.2 Memory board configuration table 346
16.2.3 Expansion card configuration table 346

16.3 Connectors and indicators 347
16.3.1 Connectors and indicators on the system board 347
16.3.1.1 Onboard connectors 347
16.3.1.2 Onboard indicators and controls 349
16.3.2 Connectors and indicators on the I/O panel 350
16.3.2.1 I/O panel connectors 350
16.3.2.2 I/O panel indicators 351
16.3.3 Connectors and indicators on the front panel 353
16.3.3.1 Front panel connectors 353
16.3.3.2 Front panel controls and indicators 354

16.4 Onboard settings 358

16.5 Minimum startup configuration 359

1 Introduction

This Upgrade and Maintenance Manual provides instructions for the following procedures:

- Upgrading the server configuration by adding optional hardware components
- Upgrading the server configuration by replacing existing hardware components with superior ones.
- Replacing defective hardware components

This manual focuses on on-site maintenance tasks. It is recommended to prepare each service assignment following remote diagnostics procedures, as described in the "ServerView Suite Local Service Concept (LSC)" manual (see section "Documents you need at hand" on page 31.

CAUTION!

The document at hand comprises procedures of a wide range of complexity. Check the profile of qualification for technicians before assigning tasks. Before you start, carefully read "Classification of procedures" on page 25.

1.1 Notational conventions

The following notational conventions are used in this manual:

Text in italics	indicates commands or menu items
`fixed font`	indicates system output
`semi-bold fixed font`	indicates text to be entered by the user
"Quotation marks"	indicate names of chapters and terms that are being emphasized
►	describes activities that must be performed in the order shown
Abc	indicates keys on the keyboard
CAUTION!	Pay particular attention to texts marked with this symbol! Failure to observe this warning may endanger your life, destroy the system or lead to the loss of data.
	indicates additional information, notes and tips
	indicates the procedure category in terms of complexity and qualification requirements, see "Classification of procedures" on page 25
	indicates the average task duration, see "Average task duration" on page 27

2 Before you start

Before you start any upgrade or maintenance task, please proceed as follows:

- Carefully read the safety instructions in chapter "Important information" on page 35.
- Make sure that all necessary manuals are available. Refer to the documentation overview in section "Documents you need at hand" on page 31. Print the PDF files if required.
- Make yourself familiar with the procedure categories introduced in section "Classification of procedures" on page 25.
- Ensure that all required tools are available according to section "Tools you need at hand" on page 28.

CAUTION

In a system that has the Cool-safe® Advanced Thermal Design option, only components that support the higher operating range may be installed. Further information on this is available in the configurator.

The Cool-safe® Advanced Thermal Design option can only be ordered from the manufacturer and is indicated by the logo on the identification rating plate.

Installing optional components

The operating manual of your server gives an introduction to server features and provides an overview of available hardware options.

Use the Fujitsu ServerView Suite management software and the iRMC web frontend to prepare hardware expansions. ServerView Suite documentation is available online at *http://manuals.ts.fujitsu.com* (*http://jp.fujitsu.com/platform/server/primergy/manual/* for the Japanese market). Please refer to the following ServerView Suite topics:

– Operation
– Virtualization
– Maintenance
– Out-Of-Band Management

For the latest information on hardware options, refer to your server's hardware configurator available online at the following address:
for the EMEA market:
http://ts.fujitsu.com/products/standard_servers/index.htm
for the Japanese market:
http://jp.fujitsu.com/platform/server/primergy/system/

Please contact your local Fujitsu customer service partner for details on how to order expansion kits or spare parts. Use the Fujitsu Illustrated Spares Catalog to identify the required spare part and obtain technical data and order information. Illustrated Spares catalogs are available online at *http://manuals.ts.fujitsu.com/illustrated_spares* (EMEA market only).

Replacing a defective component

The global error indicators on the front and rear sides of your server as well as local diagnostic LEDs on the front panel report defective hardware components that need to be replaced. For further information on the controls and indicators of your server, refer to the operating manual of your server and section "Connectors and indicators" on page 347.

If the system has been powered off in order to replace a non-hot plug unit, a system of PRIMERGY diagnostic indicators guides you to the defective component. For further information, please refer to sections "Using diagnostics information" on page 47 and "Connectors and indicators on the front panel" on page 353.

If the defective component is a customer replaceable unit included in the CSS concept (Customer Self Service, only available for EMEA market), the CSS indicators on the front and rear side of the server will light up.

For further information, refer to the "ServerView Suite Local Service Concept (LSC)" manual available online at *http://manuals.ts.fujitsu.com* (EMEA market) or *http://jp.fujitsu.com/platform/server/primergy/manual/* (Japanese market).

It is recommended to prepare local maintenance tasks using remote diagnostics procedures, as described in the "ServerView Suite Local Service Concept (LSC)" manual.

2.1 Classification of procedures

The complexity of maintenance procedures varies significantly. Procedures have been assigned to one of three unit categories, indicating the level of difficulty and required qualification.

At the beginning of each procedure, the involved unit type is indicated by one of the symbols introduced in this section.

Please ask your local Fujitsu service center for more detailed information.

2.1.1 Customer Replaceable Units (CRU)

Customer Replaceable Unit (CRU)

Customer Replaceable Units are intended for customer self service and may be installed or replaced as hot-plug components during operation.

Components that the customer is entitled to replace may differ according to the service form in his country.

Hot-plug components increase system availability and guarantee a high degree of data integrity and fail-safe performance. Procedures can be carried out without shutting down the server or going offline.

Components that are handled as Customer Replaceable Units

- Hot-plug power supply units
- Hot-plug fan modules
- Hot-plug HDD / SSD modules

Peripherals that are handled as Customer Replaceable Units

- Keyboard
- Mouse

2.1.2 Upgrade and Repair Units (URU)

Upgrade and Repair Unit (URU)

Upgrade and Repair Units are non hot-plug components that can be ordered separately to be installed as options (*Upgrade Units*) or are available to the customer through customer self service (*Repair Units*).

Server management error messages and diagnostic indicators on the front panel and system board will report defective *Upgrade and Repair Units* as customer replaceable CSS components.

Upgrade and repair procedures involve shutting down and opening the server.

CAUTION!

The device may be seriously damaged or cause damage if it is opened without authorization or if repairs are attempted by unauthorized and untrained personnel.

Components that are handled as Upgrade Units

– Processors (upgrade kits)
– Optical disk drives
– Backup drives
– Expansion cards
– Battery backup units
– Memory modules
– Front VGA module

Components that are handled solely as Repair Units

– CMOS battery

2.1.3 Field Replaceable Units (FRU)

Field Replaceable Unit (FRU)

Removing and installing *Field Replaceable Units* involves complex maintenance procedures on integral server components. Procedures will require shutting down, opening and disassembling the server.

CAUTION!

Maintenance procedures involving *Field Replaceable Units* must be performed exclusively by Fujitsu service personnel or technicians trained by Fujitsu. Please note that unauthorized interference with the system will void the warranty and exempt the manufacturer from all liability.

Components that are handled as Field Replaceable Units

- Processor (replacement)
- SAS / SATA backplanes
- Power distribution board
- Front panel module
- Management and diagnostics modules
- System board
- Standard power supply unit
- Trusted Platform Module (TPM)
- USB Flash Module (UFM)

2.2 Average task duration

Hardware: 10 minutes

The average task duration including preliminary and concluding steps is indicated at the beginning of each procedure next to the procedure class.

Refer to table 1 on page 28 for an overview of steps taken into account for calculating the average task duration:

Step	included	Explanation
Server shutdown	no	Shutdown time depends on hardware and software configuration and may vary significantly. Software tasks necessary before maintenance are described in section "Starting the maintenance task" on page 65".
Rack removal, disassembly	**yes**	Making the server available, removing the server from the rack (if applicable)
Transport	no	Transporting the server to the service table (where required) depends on local customer conditions.
Maintenance procedures	**yes**	Maintenance procedures including preliminary and concluding software tasks
Transport	no	Returning the server to its installation site (where required) depends on local customer conditions.
Assembly, rack installation	**yes**	Reassembling the server, installing the server in the rack (if applicable)
Starting up	no	Booting time depends on hardware and software configuration and may vary significantly.

Table 1: Calculation of the average task duration

2.3 Tools you need at hand

When preparing the maintenance task, ensure that all required tools are available according to the overview below. You will find a list of required tools at the beginning of each procedure.

Screw driver / Bit insert / torque	Screw	Usage	Type
Hexagonal cross SW5 0.6 Nm		HDD cages to chassis, Multibay and Panelhousing Slot bracket to chassis, Fan box	M3 x 4.5 mm (silver) C26192-Y10-C67
hexagonal cross SW5 0.6 Nm		System board, Front panel	M3 x 6 mm (silver) C26192-Y10-C68
Phillips PH0 / (+) No. 0 0.4 Nm		2.5-inch HDD/SSDs RDX in 2.5-inch variant LTO drive	M3 x 3.5 mm (silver) C26192-Y10-C102
TPM bit insert Dedicated TPM screw driver / TPM module fixing tool (for the Japanese market) 0.4 Nm		TPM screw One way head	REM 3 x 15 mm (black) C26192-Y10-C176
Hexagonal cross SW5 0.4 Nm		Slot bracket to controller board	M3 x 3.5 mm C26192-Y10-C151

Table 2: List of required tools and used screws

Screw driver / Bit insert / torque	Screw	Usage	Type
Cross 0.2 Nm		ODD latch (delivered with the accessory pack)	M2 x 5 mm (silver) C26192-Y10-C63
Cylinder head Torx Plus 6 0.2 Nm		ODD latch (used by factory mounting)	M2 x 4 mm (black) C26192-Y10-C166
Phillips PH0 / (+) No. 0 0.06 Nm		UFM nylon screw	M3 x 4.5 mm (white) A3C40109082
Phillips PH2 / (+) No. 2 0.6 Nm		USB 3.0 PCI card D3305	M3 x 5 mm (silver) (contained in card kit S26361-D3305-A10)
Philips PH1 0.4 Nm		TFM	M2.5 x 4 mm

Table 2: List of required tools and used screws

Screw driver / Bit insert / torque	Screw	Usage	Type
Hexagon bolt SW5 0.6 Nm		Front VGA	UNC 4-40
Phillips PH2 / (+) No. 2 SW6 1 Nm		heat sink	captive screw

Table 2: List of required tools and used screws

2.4 Documents you need at hand

Maintenance procedures may include references to additional documentation. When preparing the maintenance task, ensure that all required manuals are available according to the overview below.

– Ensure to store all printed manuals enclosed with your server in a save place for future reference.

– Unless stated otherwise, all manuals are available online at *http://manuals.ts.fujitsu.com* under *Industry standard servers*.

  For the Japanese market please use the following address: *http://jp.fujitsu.com/platform/server/primergy/manual/*

Document	Description
"Quick Start Hardware - FUJITSU Server PRIMERGY RX2520 M1" leaflet	Quick installation poster for initial operation, available online
"ServerView Quick Start Guide" "ServerView クイックスタートガイド " for the Japanese market	Information on initial server setup and software configuration, available online

Table 3: Documentation you need at hand

Document	Description
"Safety notes and regulations" manual "安全上のご注意" for the Japanese market	Important safety information, available online or as a printed copy
"FUJITSU Server PRIMERGY RX2520 M1" Operating Manual	Available online
"D3169 BIOS Setup Utility for FUJITSU Server PRIMERGY RX2520 M1" Reference Manual	Information on configurable BIOS options and parameters, available online
System board and service labels	Labels inside the housing cover outlining connectors, indicators and jumper
Software documentation	– "ServerView Suite Local Service Concept (LSC)" user guide – "ServerView Operations Manager - Server Management" user guide – "IRMC S4 Integrated Remote Management Controller" user guide
Illustrated Spares catalog	Spare parts identification and information system (EMEA market only), available for online use or download (Windows OS) at *http://manuals.ts.fujitsu.com/illustrated_spares* or from the CSS component view of the ServerView Operations Manager
Glossary	available online
"Warranty" manual "保証書" for the Japanese market	Important information on warranty regulations, recycling and service, available online, or as a printed copy
"Returning used devices" manual	Recycling and contact information, available online, or as a printed copy
"Service Desk" leaflet " サポート＆サービス " for the Japanese market	

Table 3: Documentation you need at hand

Document	Description
Additional documentation	– "iRMC S4" user guide available online – RAID documentation, available online at *http://manuals.ts.fujitsu.com* under *Industry standard servers - Expansion Cards - Storage Adapters* For the Japanese market please use the following address: *http://jp.fujitsu.com/platform/server/primergy/manual/* – Rack documentation
Third party documentation	– Operating system documentation, online help – Peripherals documentation

Table 3: Documentation you need at hand

3 Important information

CAUTION!

Before installing and starting up a device, please observe the safety instructions listed in the following section. This will help you to avoid making serious errors that could impair your health, damage the device and endanger the data base.

Keep this manual and the other documentation (such as the technical manual, documentation DVD) close to the device. All documentation must be included if the equipment is passed on to a third party.

3.1 Safety instructions

The following safety instructions are also provided in the manual "Safety Notes and Regulations" or " 安全上のご注意 ".

This device meets the relevant safety regulations for IT equipment. If you have any questions about whether you can install the server in the intended environment, please contact your sales outlet or our customer service team.

- The actions described in this manual shall be performed by technical specialists. A technical specialist is a person who is trained to install the server including hardware and software.
- Repairs to the device that do not relate to CSS failures shall be performed by service personnel. Please note that unauthorized interference with the system will void the warranty and exempt the manufacturer from all liability.
- Any failure to observe the guidelines in this manual, and any improper repairs could expose the user to risks (electric shock, energy hazards, fire hazards) or damage the equipment.
- Before installing/removing internal options to/from the server, turn off the server, all peripheral devices, and any other connected devices. Also unplug all power cords from the power outlet. Failure to do so can cause electric shock or damage.

Before starting up

- During installation and before operating the device, observe the instructions on environmental conditions for your device.

- If the device is brought in from a cold environment, condensation may form both inside and on the outside of the device.

  Wait until the device has acclimatized to room temperature and is absolutely dry before starting it up. Material damage may be caused to the device if this requirement is not observed.

- Transport the device only in the original packaging or in packaging that protects it from knocks and jolts.
  For the Japanese market, transporting the device in its original packaging does not apply.

Installation and operation

- This unit should not be operated in ambient temperatures above 35 °C. For servers with Cool-safe® Advanced Thermal Design the ambient temperature can increase to 40 °C.
- If the unit is integrated into an installation that draws power from an industrial power supply network with an IEC309 connector, the power supply's fuse protection must comply with the requirements for non-industrial power supply networks for type A connectors.
- The unit automatically adjusts itself to a mains voltage in a range of 100 VAC to 240 VAC. Ensure that the local mains voltage lies within these limits.
- This device must only be connected to properly grounded power outlets or connected to the grounded rack internal power distribution system with tested and approved power cords.
- Ensure that the device is connected to a properly grounded power outlet close to the device.
- Ensure that the power sockets on the device and the properly grounded power outlets are easily accessible.
- The On/Off button or the main power switch (if present) does not isolate the device from the mains power supply. In case of repair or servicing disconnect the device completely from the mains power supply, unplug all power plugs from the properly grounded power outlets.
- Always connect the server and the attached peripherals to the same power circuit. Otherwise you run the risk of losing data if, for example, the server is still running but a peripheral device (e.g. memory subsystem) fails during a power outage.
- Data cables must be adequately shielded.

- Ethernet cabling has to comply with EN 50173 and EN 50174-1/2 standards or ISO/IEC 11801 standard respectively. The minimum requirement is a Category 5 shielded cable for 10/100 Ethernet, or a Category 5e cable for Gigabit Ethernet.
- Route the cables in such a way that they do not create a potential hazard (make sure no-one can trip over them) and that they cannot be damaged. When connecting the server, refer to the relevant instructions in this manual.
- Never connect or disconnect data transmission lines during a storm (risk of lightning hazard).
- Make sure that no objects (e.g. jewelry, paperclips etc.) or liquids can get inside the server (risk of electric shock, short circuit).
- In emergencies (e.g. damaged casing, controls or cables, penetration of liquids or foreign bodies), contact the system administrator or your customer service team. Only disconnect the system from the mains power supply if there is no risk of harming yourself.
- Proper operation of the system (in accordance with IEC 60950-1 resp. EN 60950-1) is only ensured if the casing is completely assembled and the rear covers for the installation slots have been fitted (electric shock, cooling, fire protection, interference suppression).
- Only install system expansions that satisfy the requirements and rules governing safety and electromagnetic compatibility and those relating to telecommunication terminals. If you install other expansions, they may damage the system or violate the safety regulations. Information on which system expansions are approved for installation can be obtained from our customer service center or your sales outlet.
- The components marked with a warning notice (e.g. lightning symbol) may only be opened, removed or exchanged by authorized, qualified personnel. Exception: CSS components can be replaced.
- The warranty is void if the server is damaged during installation or replacement of system expansions.
- Only set screen resolutions and refresh rates that are specified in the operating manual for the monitor. Otherwise, you may damage your monitor. If you are in any doubt, contact your sales outlet or customer service center.
- Before installing/removing internal options to/from the server, turn off the server, all peripheral devices, and any other connected devices. Also unplug all power cords from the outlet. Failure to do so can cause electric shock.

- Do not damage or modify internal cables or devices. Doing so may cause a device failure, fire, or electric shock and will void the warranty and exempt the manufacturer from all liability.
- Devices inside the server remain hot after shutdown. Wait for a while after shutdown before installing or removing internal options.
- The circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. To ensure reliable protection, if you are wearing an earthing band on your wrist when working with this type of module, connect it to an unpainted, conducting metal part of the system.
- Do not touch the circuitry on boards or soldered parts. Hold the metallic areas or the edges of the circuit boards.
- Install the screw removed during installation/detaching internal options in former device/position. To use a screw of the different kind can cause a breakdown of equipment.
- The installation indicated on this document is sometimes changed to the kind of possible options without notice.

Batteries

- Incorrect replacement of batteries may lead to a risk of explosion. The batteries may only be replaced with identical batteries or with a type recommended by the manufacturer.
- Do not throw batteries into the trash can.
- Batteries must be disposed of in accordance with local regulations concerning special waste.
- Make sure that you insert the battery the right way round.
- The battery used in this device may present a fire or chemical burn hazard if mistreated. Do not disassemble, heat about 100 °C (212F), or incinerate the battery.
- All batteries containing pollutants are marked with a symbol (a crossed-out garbage can). In addition, the marking is provided with the chemical symbol of the heavy metal decisive for the classification as a pollutant:

  Cd Cadmium
  Hg Mercury
  Pb Lead

Working with optical disk drives and media

When working with optical disk drives, these instructions must be followed.

CAUTION!

- Only use CDs/DVDs/BDs that are in perfect condition, in order to prevent data loss, equipment damage and injury.
- Check each CD/DVD/BD for damage, cracks, breakages etc. before inserting it in the drive.

  Note that any additional labels applied may change the mechanical properties of a CD/DVD/BD and cause imbalance and vibrations.

  Damaged and imbalanced CDs/DVDs/BDs can break at high drive speeds (data loss).

  Under certain circumstances, sharp CD/DVD/BD fragments can pierce the cover of the optical disk drive (equipment damage) and can fly out of the device (danger of injury, particularly to uncovered body parts such as the face or neck).
- High humidity and airborne dust levels are to be avoided. Electric shocks and/or server failures may be caused by liquids such as water, or metallic items, such as paper clips, entering a drive.
- Shocks and vibrations are also to be avoided.
- Do not insert any objects other than the specified CDs/DVDs/BDs.
- Do not pull on, press hard, or otherwise handle the CD/DVD/BD tray roughly.
- Do not disassemble the optical disk drive.
- Before use, clean the optical disk tray using a soft, dry cloth.
- As a precaution, remove disks from the optical disk drive when the drive is not to be used for a long time. Keep the optical disk tray closed to prevent foreign matter, such as dust, from entering the optical disk drive.
- Hold CDs/DVDs/BDs by their edges to avoid contact with the disk surface.

- Do not contaminate the CD/DVD/BD surface with fingerprints, oil, dust, etc. If dirty, clean with a soft, dry cloth, wiping from the center to the edge. Do not use benzene, thinners, water, record sprays, antistatic agents, or silicone-impregnated cloth.
- Be careful not to damage the CD/DVD/BD surface.
- Keep the CDs/DVDs/BDs away from heat sources.
- Do not bend or place heavy objects on CDs/DVDs/BDs.
- Do not write with ballpoint pen or pencil on the label (printed) side.
- When a CD/DVD/BD is moved from a cold place to a warm place, moisture condensation on the CD/DVD/BD surface can cause data read errors. In this case, wipe the CD/DVD/BD with a soft, dry cloth then let it air dry. Do not dry the CD/DVD/BD using devices such as a hair dryer.
- To avoid dust, damage, and deformation, keep the CD/DVD/BD in its case whenever it is not in use.
- Do not store CDs/DVDs/BDs at high temperatures. Areas exposed to prolonged direct sunlight or near heating appliances are to be avoided.

You can prevent damage from the optical disk drive and the CDs/DVDs/BDs, as well as premature wear of the disks, by observing the following suggestions:

- Only insert disks in the drive when needed and remove them after use.
- Store the disks in suitable sleeves.
- Protect the disks from exposure to heat and direct sunlight.

Laser information

The optical disk drive complies with IEC 60825-1 laser class 1.

CAUTION!

The optical disk drive contains a light-emitting diode (LED), which under certain circumstances produces a laser beam stronger than laser class 1. Looking directly at this beam is dangerous.

Never remove parts of the optical disk drive casing!

Modules with Electrostatic-Sensitive Devices

Modules with electrostatic-sensitive devices are identified by the following sticker:

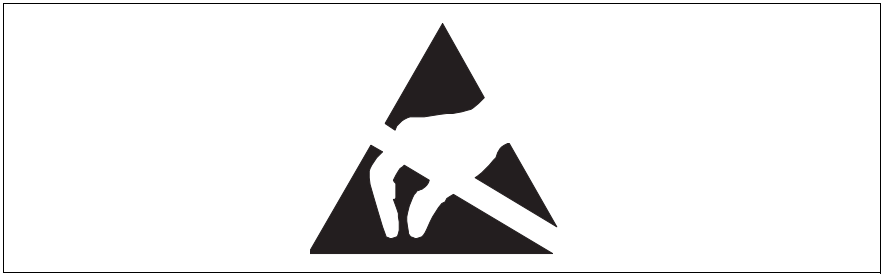


Figure 1: ESD label

When you handle components fitted with ESDs, you must always observe the following points:

- Switch off the system and remove the power plugs from the power outlets before installing or removing components with ESDs.
- The circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. To ensure reliable protection, you must wear an earthing band on your wrist when working with this type of module and connect it to an unpainted, conducting metal part of the system.
- Any devices or tools that are used must be free of electrostatic charge.
- Wear a suitable grounding cable that connects you to the external chassis of the system unit.
- Always hold components with ESDs at the edges or at the points marked green (touch points).
- Do not touch any connectors or conduction paths on an ESD.
- Place all the components on a pad which is free of electrostatic charge.

For a detailed description of how to handle ESD components, see the relevant European or international standards (EN 61340-5-1, ANSI/ESD S20.20).

Transporting the server

- Only transport the server in its original packaging or in packaging that protects it from impacts and jolts.
  For the Japanese market, transporting the device in its original packaging does not apply.
- Do not unpack the server until it is at its installation location.
- If you need to lift or transport the server, ask other people to help you. Because the PRIMERGY RX2520 M1 is large and heavy, at least two people are needed.
- Never lift or carry the device by the handles on the front panel.

Notes on installing the server in the rack

- **For safety reasons, at least two people are required to install the server in the rack because of its weight and size.**

  (For the Japanese market, please refer to " 安全上のご注意 ".)
- Never lift the server into the rack using the handles on the front panel.
- When connecting and disconnecting cables, observe the relevant instructions in the "Important Information" chapter of the technical manual for the corresponding rack. The technical manual is supplied with the corresponding rack.
- When installing the rack, make sure that the anti-tilt protection is correctly fitted.
- For safety reasons, no more than one unit may be removed from the rack at any one time during installation and maintenance work.
- If several units are simultaneously removed from the rack, there is a risk that the rack could tip over.
- The rack must be connected to the power supply by an authorized specialist (electrician).
- If the server is integrated into an installation that draws power from an industrial power supply network with an IEC309 type connector, the power supply's fuse protection must comply with the requirements for non-industrial power supply networks for the type A connector.

3.2 ENERGY STAR

Products that have been certified compliant with ENERGY STAR and identified as such are in full compliance with the specification at shipping. Note that energy consumption can be affected by software that is installed or any changes that are made to the hardware configuration or BIOS or energy options subsequently. In such cases, the properties guaranteed by ENERGY STAR can no longer be assured.

The "ServerView Operations Manager" user guide contains instructions for reading out measurement values, including those relating to current energy consumption and air temperatures. Either the Performance Monitor or the Task Manager can be used to read out CPU utilization levels.

3.3 CE conformity

The system complies with the requirements of the EC directives 2004/108/EC regarding "Electromagnetic Compatibility" and 2006/95/EC "Low Voltage Directive" and the directive of the European Parliament and Council 2011/65/EU. This is indicated by the CE marking (CE = Communauté Européenne).

3.4 FCC Class A Compliance Statement

If there is an FCC statement on the device, it applies to the products covered in this manual, unless otherwise specified herein. The statement for other products will appear in the accompanying documentation.

NOTE:

This equipment has been tested and found to comply with the limits for a "Class A" digital device, pursuant to Part 15 of the FCC rules and meets all requirements of the Canadian Interference-Causing Equipment Standard ICES-003 for digital apparatus. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in strict accordance with the instructions, may cause harmful interference to radio communications. However, there is no warranty that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Fujitsu is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Fujitsu. The correction of interferences caused by such unauthorized modification, substitution or attachment will be the responsibility of the user.

The use of shielded I/O cables is required when connecting this equipment to any and all optional peripheral or host devices. Failure to do so may violate FCC and ICES rules.

WARNING:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

3.5 Environmental protection

Environmentally-friendly product design and development

This product has been designed in accordance with the Fujitsu standard for "environmentally friendly product design and development". This means that key factors such as durability, selection and labeling of materials, emissions, packaging, ease of dismantling and recycling have been taken into account.

This saves resources and thus reduces the harm done to the environment. Further information can be found at:

– *http://ts.fujitsu.com/products/standard_servers/index.html* (for the EMEA market)
– *http://jp.fujitsu.com/platform/server/primergy/concept/* (for the Japanese market)

Energy-saving information

Devices that do not need to be constantly switched on should be switched off until they are needed as well as during long breaks and after completion of work.

Packaging information

This packaging information doesn’t apply to the Japanese market.

Do not throw away the packaging. You may need it later for transporting the system. If possible, the equipment should only be transported in its original packaging.

Information on handling consumables

Please dispose of printer consumables and batteries in accordance with the applicable national regulations.

In accordance with EU directives, batteries must not be disposed of with unsorted domestic waste. They can be returned free of charge to the manufacturer, dealer or an authorized agent for recycling or disposal.

All batteries containing pollutants are marked with a symbol (a crossed-out garbage can). They are also marked with the chemical symbol for the heavy metal that causes them to be categorized as containing pollutants:

Cd Cadmium
Hg Mercury
Pb Lead

Labels on plastic casing parts

Please avoid sticking your own labels on plastic parts wherever possible, since this makes it difficult to recycle them.

Returns, recycling and disposal

Please handle returns, recycling and disposal in accordance with local regulations.

The device must not be disposed of with domestic waste. This device is labeled in compliance with European directive 2002/96/EC on waste electrical and electronic equipment (WEEE).

This directive sets the framework for returning and recycling used equipment and is valid across the EU. When returning your used device, please use the return and collection systems available to you. Further information can be found at *http://ts.fujitsu.com/recycling*.

Details regarding the return and recycling of devices and consumables within Europe can also be found in the "Returning used devices" manual, via your local Fujitsu branch or from our recycling center in Paderborn:

Fujitsu Technology Solutions
Recycling Center
D-33106 Paderborn

Tel. +49 5251 525 1410
Fax +49 5251 525 32 1410

4 Basic hardware procedures

4.1 Using diagnostics information

Use the Fujitsu ServerView Suite management software to plan the upgrade or replacement of hardware components. Please refer to the following ServerView Suite topics:

– Operation
– Maintenance

It is recommended to prepare local maintenance tasks using remote diagnostics procedures, as described in the "ServerView Suite Local Service Concept (LSC)" manual.

Please contact your local Fujitsu customer service partner for details on the service concept and on how to order expansion kits or spare parts. Use the Fujitsu Illustrated Spares Catalog to identify the required spare part and obtain technical data and order information. Illustrated Spares catalogs are available online at *http://manuals.ts.fujitsu.com/illustrated_spares* (EMEA market only).

Perform the following diagnostics procedures to identify defective servers and components.

4.1.1 Locating the defective server

When working in a datacenter environment, switch on the ID indicator on the front and rear connector panels of the server for easy identification.

► Press the ID button on the front panel, use the iRMC web frontend or use the ServerView Operations Manager user interface to switch on the system identification LEDs.

For further information, refer to the "ServerView Suite Local Service Concept (LSC)" manual I and "Integrated Remote Management Controller" user guide.

► When using ServerView Operations Manager to toggle the ID indicator, choose *Single System View* and press the *Locate* button.

► Remember to switch off the ID indicator after the maintenance task has been concluded successfully.

4.1.2 Determining the error class

The Local Service Concept (LSC) allows you to identify defective server components. Failure events are assigned to one of two error classes:

– **Global Error** events that need to be resolved by maintenance personnel

– **Customer Self Service** (CSS) error events that may be resolved by operating personnel

Global Error and CSS LEDs indicate, if the defective component is a customer replaceable unit or if maintenance personnel needs to be dispatched to replace the part.

The indicators also light up in standby mode and after a server restart due to a power failure.

4.1.2.1 Global Error indicator

► Check the Global Error indicator on the front or connector panel of the server:

► For further diagnostics, proceed as follows:

– Hardware errors:

  Check the System Event Log (SEL) as described in section "Viewing the SEL" on page 85.

– Software / agent related errors:

  Check the ServerView System Monitor, available on Windows or Linux based servers with ServerView agents installed.

  For further information, please refer to the "ServerView System Monitor" user guide.

4.1.2.2 Customer Self Service (CSS) indicator

► Check the CSS indicator on the front panel or connector panel of the server:

4.1.3 Locating the defective component

After determining the error class by the CSS or Global Error indicators (see section "Determining the error class" on page 48) local diagnostic indicators on the front panel and system board allow you to identify the defective component.

For further information, refer to the "ServerView Suite Local Service Concept (LSC)" manual.

4.1.3.1 Local diagnostic indicators on the front

- Check the CSS indicator on the front and connector panels of the server:

In addition to local diagnostic indicators, CSS or Global Error LEDs indicate, if the defective component is a customer or field replaceable unit (see section "Determining the error class" on page 48).

4.2 Shutting down the server

CAUTION!

For further safety information, please refer to chapter "Important information" on page 35.

This step is only required when upgrading or replacing non-hot plug components.

- Inform the system administrator that the server will be shut down and put offline.
- Terminate all applications.
- Perform the required procedures described in the preliminary steps of each upgrade or maintenance task.
- "Verifying and configuring the backup software solution" on page 69.
- In case of Multipath I/O environments, please refer to section "Note on server maintenance in a Multipath I/O environment" on page 70.
- "Removing backup and optical disk media" on page 69.
- Shut down the server.

If the system is running an ACPI-compliant operating system, pressing the On / Off button will perform a graceful shutdown.

► Switch on the ID indicator on the front and rear connector panels of the server as described in section "Locating the defective server" on page 47.

4.3 Disconnecting power cords

Removing the server from the mains

If there are installed two power supplies remove both power cords.

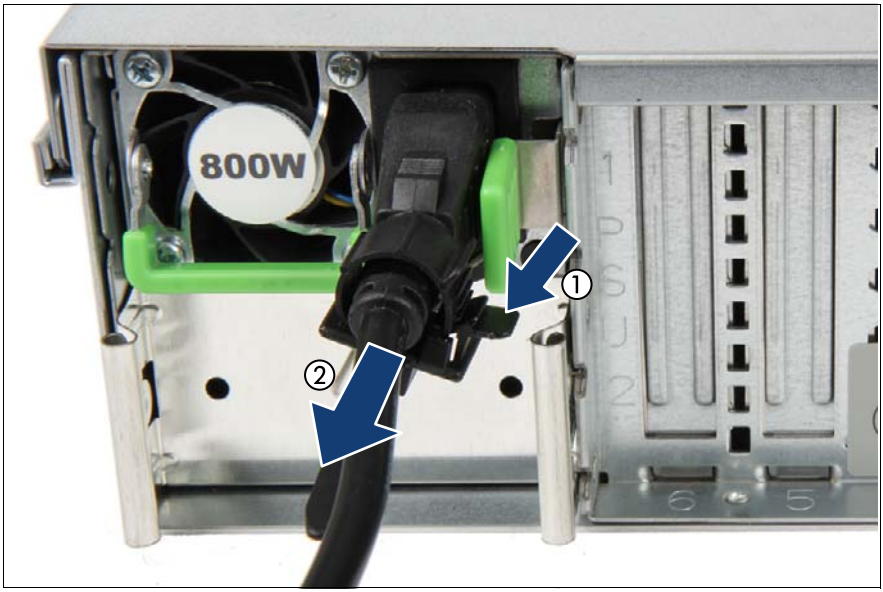


Figure 2: Removing the power cord from the PSU cable clamp

► Open on the locking lever on the PSU cable clamp (1).

► Disconnect the power cord from the PSU and remove it from the cable tie (2).

4.4 Getting access to the component

CAUTION!

- Before removing or installing covers, turn off the server and all peripheral devices. Also unplug all power cables from the outlet. Failure to do so can cause electric shock.
- In order to comply with applicable EMC regulations (regulations on electromagnetic compatibility) and satisfy cooling requirements, the server must not run while the top / side cover is removed.
- For further safety information, please refer to chapter "Important information" on page 35.

4.4.1 Extending the server out of the rack

CAUTION!

- Use the anti-tilt plate to prevent the rack from tipping when installing the rack. Pulling the server out of the rack without having installed the anti-tilt plate may cause the rack to tip over.
- Be careful not to pinch fingers or clothes when sliding out the server or pushing it back. Failure to do so may cause injury.
- For further safety information, please refer to chapter "Important information" on page 35.

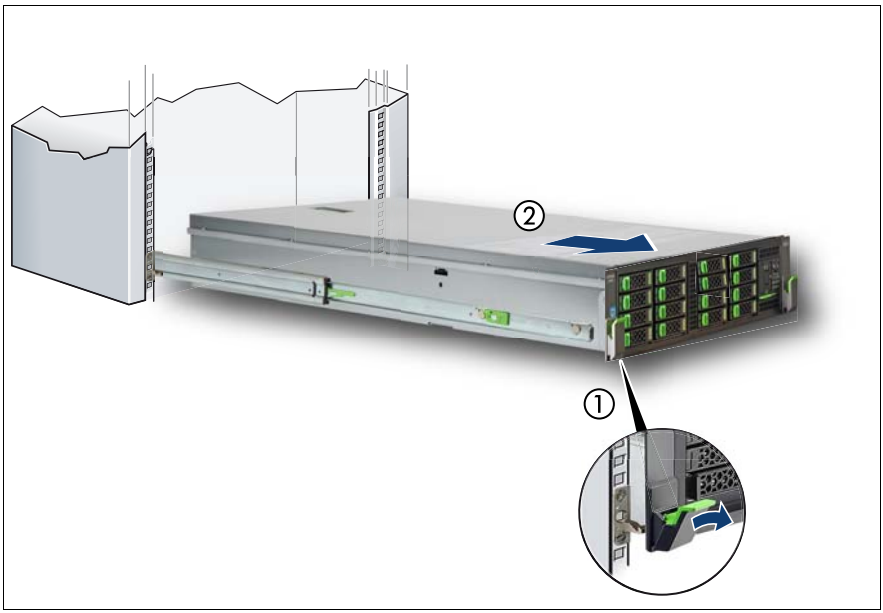


Figure 3: Extending the server out of the rack

- Remove all remaining external cables from the rear connector panel and expansion cards (see section "Connectors and indicators" on page 347).
- If you are not using a cable mounting arm (CMA kit), ensure that the rear cables are long enough not to be strained or damaged when extending the server out of the rack.
- Fold down the two quick release levers on the rack mounting frame (1) and pull the server out of the rack until it locks in place (2).

CAUTION!

Do not use the extended server as a surface on which to put things or as a work surface, and strictly avoid leaning on or against it.

4.4.2 Removing the server from the rack

In most cases maintenance tasks can be performed while the server is extended from the rack. However, depending on accessibility or security guidelines, it may make sense to completely remove the server from the rack cabinet for maintenance purposes.

CAUTION!

At least two people are needed to lift the server out of the rack cabinet. (For the Japanese market, please refer to " 安全上のご注意 ".)

For configurations below 32 kg:

At least two people are needed to lift the server out of the rack cabinet.

For configurations below 55 kg:

At least three people are needed to lift the server out of the rack cabinet.

For configurations above 55 kg:

At least four people are needed to lift the server out of the rack cabinet.

Additionally, a lifter is required in the following cases:

- The server weighs more than 50 kg.
- The server weighs more than 21 kg and is installed above the height of 25 U.

When using a lifter, this removal procedure needs to be carried out by maintenance personnel.

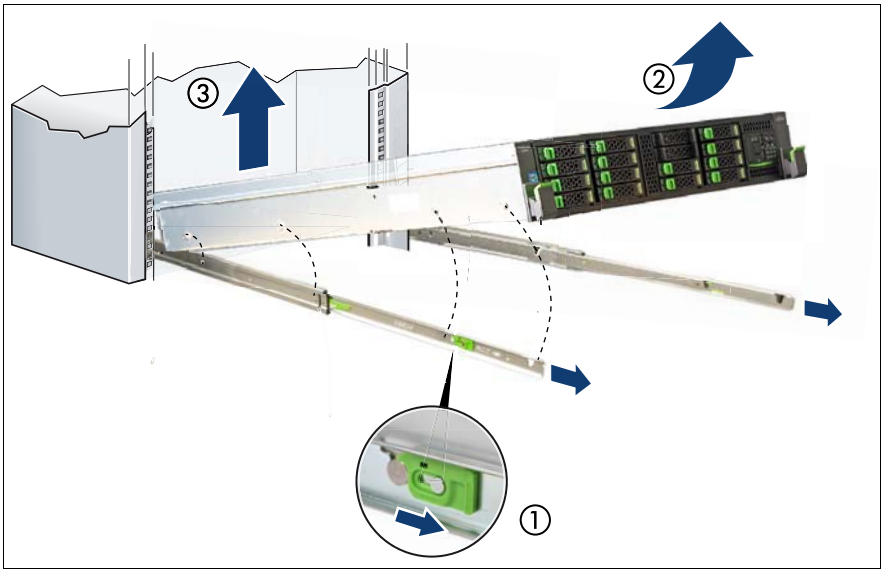


Figure 4: Removing the server from the rack

- ► Release the locking bars on both rails (1).
- ► Lift up the front of the server as shown so that the front and middle rack mounting bolts are disengaged from the mounting points on the telescopic rails (2).
- ► Lift the server out of the rear mounting points (3) and place it on an even surface.

4.4.3 Opening the server

CAUTION!

- Before removing or installing covers, turn off the server and all peripheral devices. Also unplug all power cables from the outlet. Failure to do so can cause electric shock.

- In order to comply with applicable EMC regulations (regulations on electromagnetic compatibility) and satisfy cooling requirements, the PRIMERGY RX2520 M1 server must not run while the housing cover is removed.
- For further safety information, please refer to chapter "Important information" on page 35.

4.4.3.1 Removing the housing cover

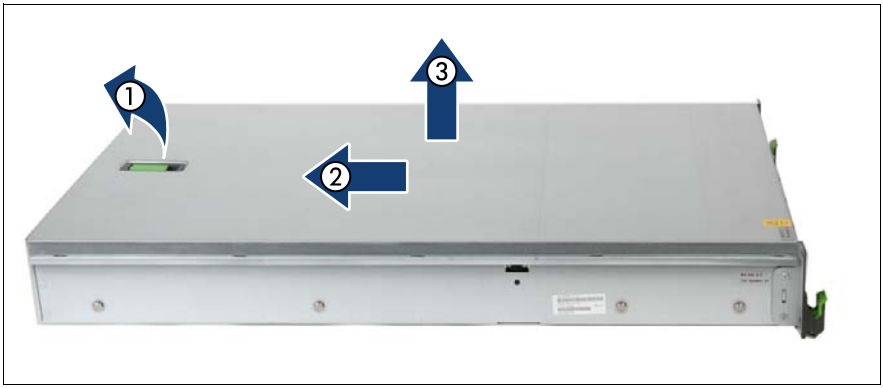


Figure 5: Removing the housing cover

► Open the locking lever (1). This will slide the top cover back disengaging the locking mechanism (2).

► Remove the top cover (3).

4.4.3.2 Removing the air duct

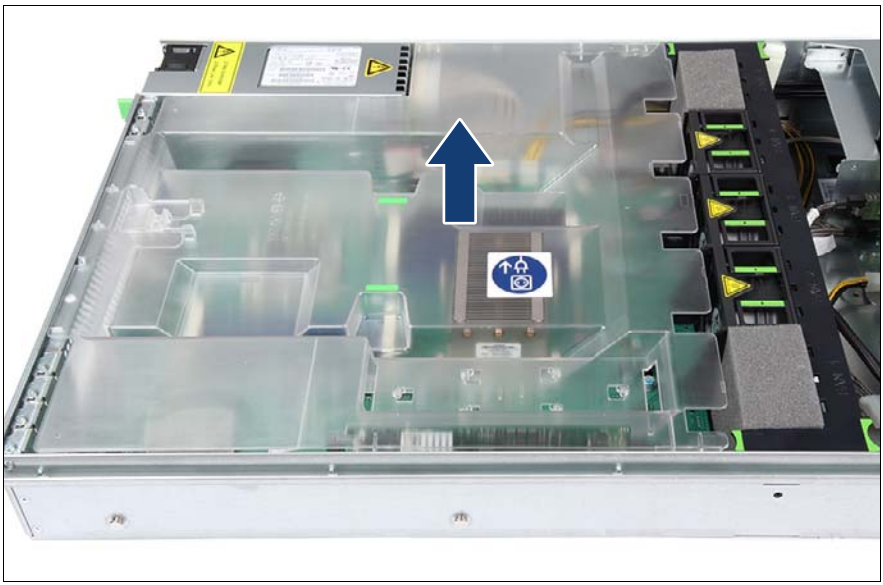


Figure 6: Removing the air duct

CAUTION!

Be careful with the FBU cable.

If there is a FBU installed, follow the procedure that is described in section "Removing the air duct with an FBU" on page 182 first.

► Remove the air duct.

4.5 Reassembling

4.5.1 Installing the air duct

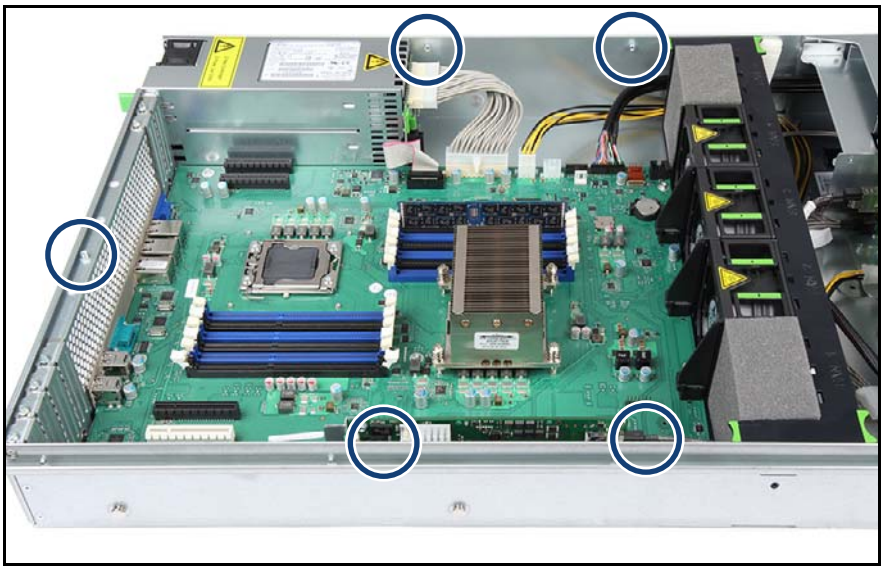


Figure 7: Installing the air duct guiding points

Regard that the air duct engages in the guiding points.

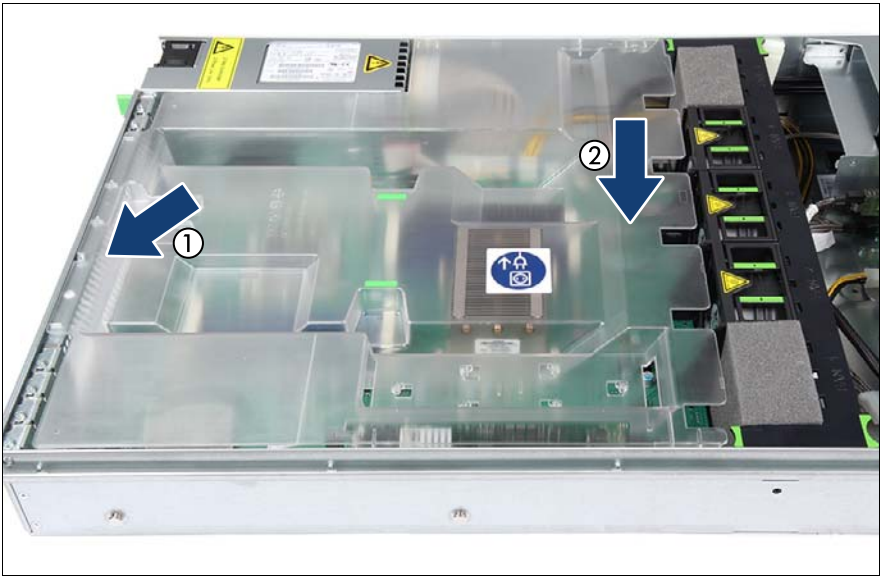


Figure 8: Installing the air duct

- ► Insert the air duct first with the rear side (1).
- ► Fold down the air duct (2).

> **i** If there is a FBU installed, follow the procedure that is described in section "Installing the air duct with an FBU" on page 180.

4.5.2 Closing the server

CAUTION!

- Before attaching the covers, make sure no unnecessary parts or tools are left inside the server.
- In order to comply with applicable EMC regulations (regulations on electromagnetic compatibility) and satisfy cooling requirements, the PRIMERGY RX2520 M1 server must not run while the housing cover is removed.
- For further safety information, please refer to chapter "Important information" on page 35.

4.5.2.1 Mounting the housing cover

Figure 9: Mounting the housing cover

- ► Open the locking lever on the top cover.
- ► Fit the housing cover on the chassis, aligning it according to the edge guide marking on the upper server surface.
- ► Lower the housing cover onto the chassis.
- ► Close the locking lever on the housing cover. This will slide the housing cover shut engaging the locking mechanism.

4.5.3 Mounting the server in the rack

4.5.3.1 Seating the server on the rack rails

CAUTION!

At least two people are needed to position the server on the rack rails. (For the Japanese market, please refer to " 安全上のご注意 ".)

For configurations below 32 kg:

At least two people are needed to lift the server into the rack cabinet.

For configurations below 55 kg:

At least three people are needed to lift the server into the rack cabinet.

For configurations above 55 kg:

At least four people are needed to lift the server into the rack cabinet.

Additionally, a lifter is required in the following cases:

– The server weighs more than 50 kg.
– The server weighs more than 21 kg and is to be installed above the height of 25 U.

When using a lifter, this installation procedure needs to be carried out by maintenance personnel.

Refer to the rack cabinet manuals for more detailed information on other support systems.

► If required, install the rack mounting bracket and rack system into the rack as described in the Rack Mounting Kit - RMK-F1/F2 DROP-IN Quick Release Lever (QRL)" Mounting Instructions.

The printed poster is contained in the rack mounting kit.

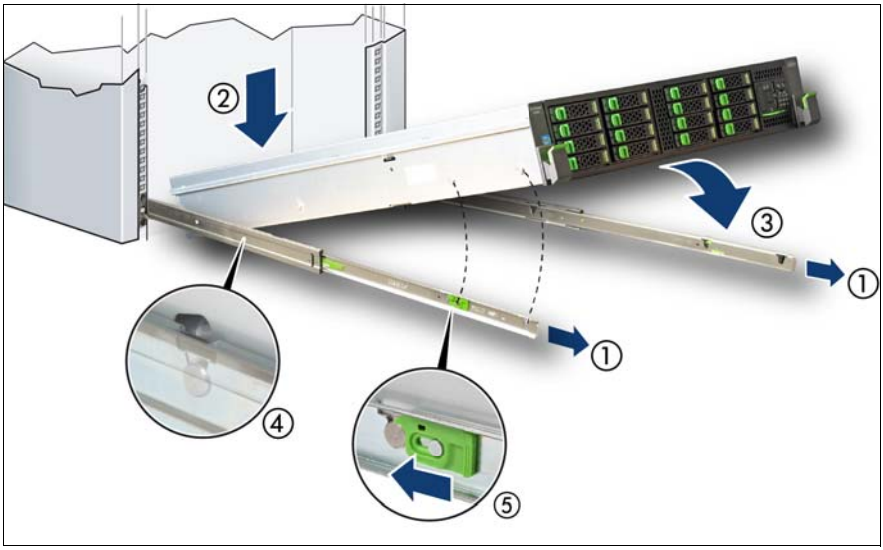


Figure 10: Mounting the server onto the rack rails

- ► Fully extend the telescopic rails until they lock in place (1).
- ► At a slight angle, lower the server onto the rear mounting point on the telescopic rails (2).
- ► Fold down the server (3). Ensure that all six rack mounting bolts are properly seated in the mounting points on the telescopic rails (4) and that the locking bars engage (5).

4.5.3.2 Sliding the server into the rack

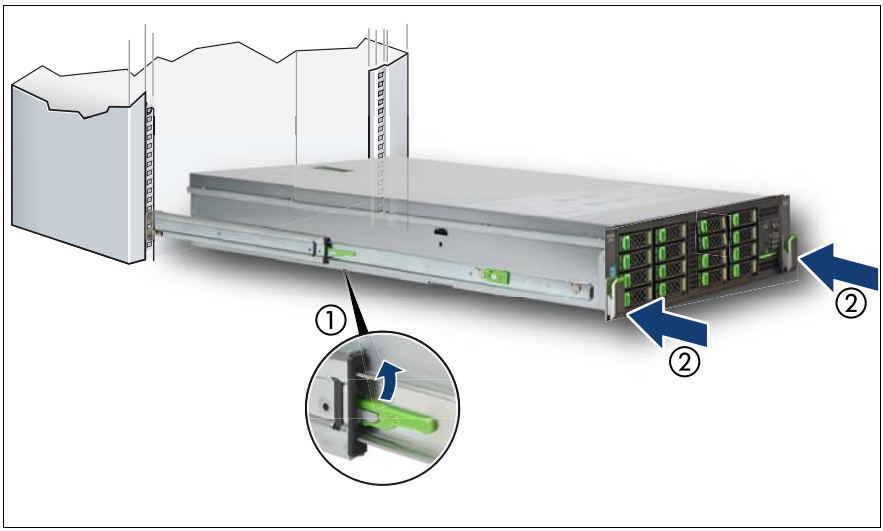


Figure 11: Sliding the server into the rack

- ► Pull up on the locking latch on both telescopic rails (1).
- ► Slide the server inside the rack as far as it will go (2) until the quick release levers on the rack mounting frame lock into place.
- ► Reconnect all cables except the power cord to the server rear.

  If you are not using a cable mounting arm (CMA kit), ensure that the rear cables are long enough not to be strained or damaged when extending the server out of the rack.

  Use cable ties to prevent loose cables from blocking the air flow.

  For information on connecting and securing the power cord, refer to section "Connecting the server to the power source" on page 62.

4.6 Connecting the server to the power source

The PRIMERGY RX2520 M1 server is equipped with up to two standard power supplies unit that automatically adjusts to any mains voltage in the range of 100 VAC to 240 VAC or up to two DC hot-plug power supply unit that adjusts automatically to any power voltage in the range from -40.5 V to -57 V.

Connecting power cords to the mains

CAUTION!

The power supply automatically adjusts to any mains voltage in the range of 100 VAC to 240 VAC. You may only operate the server if its rated voltage range corresponds to the local mains voltage.

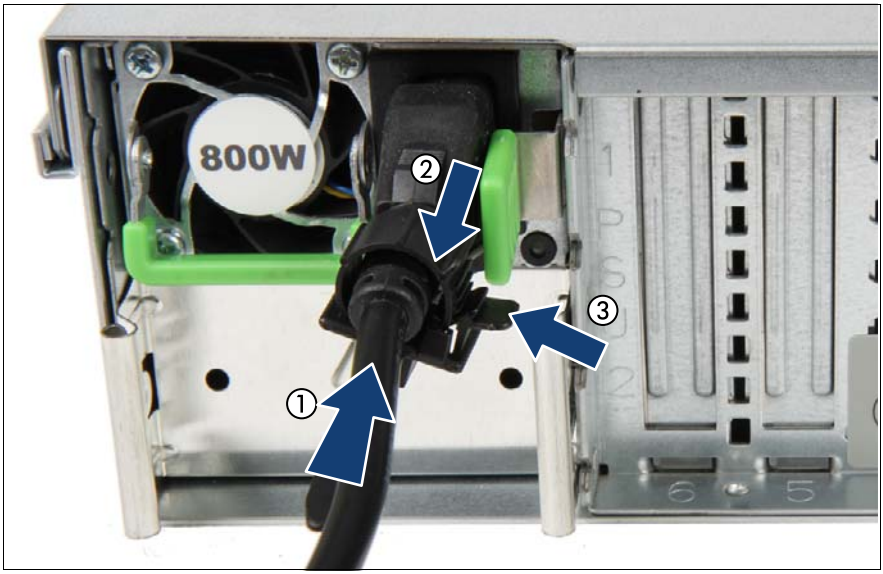


Figure 12: Securing power cord

- ► Connect the power connector (1) to the power supply unit.
- ► Close the cable clamp around the power cord (2) and lock the cable clamp (3) to secure the power cord.
- ► Connect the mains plug to a grounded mains outlet in the in-house power supply network or a power outlet of the rack socket strip (see also "PRIMECENTER Rack System" assembly guide).

To provide true phase redundancy, the second power supply should be connected to a different AC power source from the other supply. If one AC power source should fail, the server will still continue to run.

It takes about 60 seconds until power-on becomes possible.

4.7 Switching on the server

CAUTION!

- Before switching on the server, make sure the housing cover is closed. In order to comply with applicable EMC regulations (regulations on electromagnetic compatibility) and satisfy cooling requirements, the PRIMERGY RX2520 M1 server must not run while the housing cover is removed.
- After connecting all power cords, wait at least 60 seconds before pressing the On / Off button.
- Follow the safety instructions in chapter "Important information" on page 35.

► Press the On / Off button to start up the server.

► Perform the required procedures described in the concluding steps of each upgrade or maintenance task.

5 Basic software procedures

5.1 Starting the maintenance task

5.1.1 Disabling BitLocker functionality

BitLocker Drive Encryption provides protection for operating system and data drives by encrypting the contents and requiring users to authenticate their credentials to access the information. On the operating system drive, BitLocker uses the compatible Trusted Platform Module (TPM) to detect if the computer's startup process has been modified from its original state.

Disabling BitLocker Drive Encryption is a temporary method for removing BitLocker protection without decrypting the drive Windows is installed on. Disable BitLocker before modifying the server's hardware configuration or startup files. Enable BitLocker again after the maintenance procedure is complete.

CAUTION!

– With BitLocker features enabled, modifying the system configuration (hardware or firmware settings) may render the system inaccessible. The system may enter Recovery Mode and require a 48-digits recovery password to return to normal operation.

  Ensure to disable BitLocker drive encryption before maintaining the server.

– When disabled, BitLocker uses a plain text key instead of the Trusted Platform Module (TPM) to read encrypted files. Keep in mind that information on this drive is not secure until BitLocker has been re-enabled.

► Ask the system administrator to disable BitLocker-protection on the operating system drive, using the BitLocker setup wizard available either from the Control Panel or Windows Explorer:

  ► Open BitLocker Drive Encryption by clicking the *Start* button, clicking *Control Panel*, clicking *Security*, and then clicking *Bitlocker Drive Encryption*.

Administrator permission required: If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

► To temporarily disable BitLocker, click *Turn Off BitLocker*, and then click *Disable BitLocker Drive Encryption*.

In order to determine which features are accessible through the BitLocker setup wizard, modify the BitLocker Group Policy settings.

For further information on how to disable BitLocker drive encryption, please refer to the Microsoft Knowledge Base.

Fujitsu service partners will find additional information (also available in Japanese) on the Fujitsu Extranet web pages.

5.1.2 Disabling SVOM boot watchdog functionality

The ServerView Operations Manager boot watchdog determines whether the server boots within a preset time frame. If the watchdog timer expires, the system will automatically reboot.

5.1.2.1 Viewing boot watchdog settings

Viewing boot watchdog settings in the BIOS

► Enter the BIOS.

► Select the *Server Mgmt* menu.

► Under *Boot Watchdog*, you can obtain detailed information about the current watchdog status, time out intervals and actions that are triggered if watchdog time outs are exceeded.

For detailed information on BIOS settings, refer to the corresponding BIOS Setup Utility reference manual.

Viewing boot watchdog settings in the iRMC web frontend

► Enter the ServerView iRMC web frontend.

► Select the *Server Management* menu.

- Under *Watchdog Settings*, you can obtain detailed information about the current watchdog status, time out intervals and actions that are triggered if watchdog time outs are exceeded.

For detailed information on iRMC settings, refer to the "Integrated Remote Management Controller" user guide.

Viewing boot watchdog settings in ServerView Operations Manager

- In ServerView Operations Manager *Single System View* select *Maintenance* from the *Information / Operation* menu.
- Under *ASR&R* select the *Watchdog* tab to obtain detailed information about the current watchdog status, time out intervals and actions that are triggered if watchdog time outs are exceeded.

For more detailed information, refer to the "ServerView Operations Manager - Server Management" user guide.

5.1.2.2 Configuring boot watchdog settings

If the system is to be started from removable boot media for firmware upgrade purposes, the Boot watchdog needs to be disabled before starting maintenance task. Otherwise, the Boot watchdog might initiate a system reboot before the flash process is complete.

CAUTION!

An incomplete firmware upgrade process may render the server inaccessible or result in damaged / destroyed hardware.

Timer settings can be configured in the BIOS or using the ServerView iRMC web frontend:

Configuring boot watchdog settings in the BIOS

- Enter the BIOS.
- Select the *Server Mgmt* menu.
- Under *Boot Watchdog* set the *Action* setting to *Continue*.
- Save your changes and exit the BIOS.

For detailed information on how to access the BIOS and modify settings, refer to the corresponding BIOS Setup Utility reference manual.

Configuring boot watchdog settings using the iRMC web frontend

- ► Enter the ServerView iRMC web frontend.
- ► Select the *Server Management* menu.
- ► Under *Watchdog Settings* select *Continue* from the *Boot Watchdog* drop down list.
- ► Click *Apply* for the changes to take effect.

For detailed information on iRMC settings, refer to the "Integrated Remote Management Controller" user guide.

5.1.3 Removing backup and optical disk media

- ► Ask the system administrator to eject all remaining backup or optical media from the backup or optical disk drive before removing it from the server.
- ► If the backup media cannot be ejected by conventional means, and it is mandatory that the cartridge be removed prior to returning the drive for repair or disposing it, a manual tape extraction needs to be performed.

  For further information on "forcible" tape ejection, please refer to the "Tape Facts" guide available to Fujitsu service partners from the following https address:

  https://partners.ts.fujitsu.com/com/service/ps/Servers/PRIMERGY/Pages/TapeFacts.aspx

  For the Japanese market, please contact Fujitsu support, if "forcible" tape ejection is necessary.

  Fujitsu does not assume responsibility for any damage to the tape drive, the data cartridge / tape or for the loss of any data resulting from manual tape extraction procedures.

5.1.4 Verifying and configuring the backup software solution

This task only applies to the Japanese market.

Depending on the backup software solution, it may be necessary to disable or delete the backup drive from the backup software drive list before starting the maintenance task.

This is the case for the following backup software solution:

– BackupExec

Procedures may differ depending on the backup software. For details, refer to the dedicated documentation provided separately.

Further information on suitable backup software solutions and related documentation is available to Fujitsu service partners from the Fujitsu Extranet pages.

5.1.5 Note on server maintenance in a Multipath I/O environment

When booting your server offline from the ServerView Suite DVD to perform an offline BIOS / firmware update using the ServerView Update DVD or collect diagnostic data using PrimeCollect in a Multipath I/O environment, there is a risk of damaging the system configuration which may leave the system unable to boot.

This is a known restriction of Windows PE with Multipath drivers.

Using Update Manager Express

- If performing an offline BIOS / firmware update, first of all prepare the ServerView Update DVD or USB stick:
  - Download the latest ServerView Update DVD image from Fujitsu:

    for the EMEA market
    ftp://ftp.ts.fujitsu.com/images/serverview

    for the Japanese market:
    http://jp.fujitsu.com/platform/server/primergy/products/note/svsdvd/dvd/
  - Burn the image to a DVD.
  - In order to create a bootable USB stick, please proceed as described in the "Local System Update for PRIMERGY Servers" user guide.
- Before using the ServerView Update DVD or USB stick in an offline environment, properly shut down the server and disconnect all external I/O connections (like LAN or FC cables) from the system. Only keep mouse, keyboard, video cable and AC power cord connected.

  Ensure that all external I/O connections are uniquely identified so that you can reconnect them into their original locations after concluding the task.

To start Update Manager Express from the (physical) Update DVD or from a USB stick, proceed as follows:

- Prepare your Update DVD or USB stick as described in the "Local System Update for PRIMERGY Servers" user guide.
- Boot the server from the prepared Update DVD or USB stick:

DVD: ► Switch on the server.

► Right after switching on the server, insert the Update DVD into the DVD drive and close the tray.

USB: ► Connect the USB stick to the server.

► Switch on the server.

If the server does not boot from DVD or USB stick, proceed as follows:

► Reboot the server, e.g. by pressing the reset button on the front or switching the server off and then on again after a few seconds.

► Once the server has been started, press F12 to enter the boot menu.

► Use the ↑ and ↓ cursor keys to select your DVD drive or USB stick as boot device and press ENTER.

The server will now boot from the Update DVD or USB stick.

► After the boot process is complete, select your preferred GUI language.

The Update Manager Express main window will be displayed.

► Finish the intended maintenance task.

i For further information, refer to the "Local System Update for PRIMERGY Servers" user guide.

Using PrimeCollect

To start PrimeCollect, proceed as follows:

► Before using PrimeCollect in an offline environment, properly shut down the server and disconnect all external I/O connections (like LAN or FC cables) from the system. Only keep mouse, keyboard, video cable and AC power cord connected.

i Ensure that all external I/O connections are uniquely identified so that you can reconnect them into their original locations after concluding the task.

► Switch on the server.

► Right after switching on the server, insert the ServerView Suite DVD into the DVD drive and close the drive tray.

If the server does not boot from DVD, proceed as follows:

- ► Reboot the server, e.g. by pressing the reset button on the front or switching the server off and then on again after a few seconds.
- ► Once the server has been started, press F12 to enter the boot menu.
- ► Use the ↑ and ↓ cursor keys to select your DVD drive as boot device and press ENTER.

The server will now boot from the ServerView Suite DVD.

- ► After the boot process is complete, select your preferred GUI language.
- ► In the initial Installation Manager startup window, choose *PrimeCollect* from the *Installation Manager mode* section.
- ► Click *Continue* to proceed.
- ► Finish the intended maintenance task.

i For further information, refer to the "PrimeCollect" user guide.

Concluding the procedure

- ► After the update or diagnostic procedure has been completed, shut down the server, reconnect all external I/O connections and bring the system back to normal operation.
- ► If necessary, perform this procedure for all remaining servers within the Multipath environment.

5.1.6 Switching on the ID indicator

When working in a datacenter environment, switch on the ID indicator on the front and rear connector panels of the server for easy identification.

i For further information, refer to section "Locating the defective server" on page 47 or to the "ServerView Suite Local Service Concept (LSC)" and "Integrated Remote Management Controller" user guides.

Using the ID button on the front panel

- ► Press the ID button on the front panel to switch on the system identification LEDs.

i For further information, refer to section "Front panel controls and indicators" on page 354.

Using the iRMC web frontend

- ► Enter the ServerView iRMC web frontend.
- ► Under *System Overview*, click *Identify LED On* to switch on the ID indicators.

Using ServerView Operations Manager

- ► In ServerView Operations Manager *Single System View* press the *Locate* button in the title bar to switch on the ID indicators.

5.2 Completing the maintenance task

5.2.1 Updating or recovering the system board BIOS and iRMC

After replacing the system board, memory or a CPU, it is essential to upgrade the BIOS and iRMC to the latest version. The latest BIOS and iRMC versions are available from the Fujitsu support internet pages at:

http://ts.fujitsu.com/support/ (EMEA market)
http://jp.fujitsu.com/platform/server/primergy/downloads/ (Japanese market)

Fujitsu does not assume responsibility for any damage done to the server or for the loss of any data resulting from BIOS updates.

5.2.1.1 Updating or recovering the system board BIOS

BIOS flash procedure

For the Japanese market, follow the instructions provided separately.

- ► Perform the BIOS flash procedure as described in your server's "BIOS Setup Utility" reference manual.

BIOS recovery procedure

For the Japanese market, follow the instructions provided separately.

- ► Perform the BIOS recovery procedure as described in your server's "BIOS Setup Utility" reference manual.

5.2.1.2 Updating or recovering the iRMC

iRMC flash procedure

For the Japanese market, follow the instructions provided separately.

- ► Prepare a USB stick including the bootable iRMC firmware update image.
- ► Connect the USB stick to the USB port.

  Ensure that only the USB device with the iRMC firmware is connected to the USB port. Remove all other USB devices temporarily.
- ► Restart the server.
- ► The system will detect the USB stick.

  If the BIOS cannot identify the USB stick, the pop-up message `Failed to boot for Emergency flash. Please Reset now.` will show up in the center of the screen.
- ► Choose one of the following options from the update tool menu to start the iRMC update process:

  Normal Choose this option to update an existing system board.

  Initial Choose this option if the system board has been replaced prior to the iRMC update procedure. This option will perform all relevant flash procedures in a row, including the iRMC firmware and bootloader.

  CAUTION!

  Do not interrupt the iRMC upgrade process after it has started. If the process is interrupted, the iRMC BIOS may be permanently corrupted.

  If the iRMC does not work after flashing, disconnect the system from the mains and reconnect it again.
- ► After completion of the flash process, remove the USB stick and restart the server.

iRMC recovery procedure

For the Japanese market, follow the instructions provided separately.

- ► Prepare a USB stick including the bootable iRMC firmware update image.

- ► Ensure that the server has been shut down and disconnected from the mains as described in section "Shutting down the server" on page 49.
- ► Connect the USB stick to the USB port.

  Ensure that only the USB device with the iRMC firmware is connected to the USB port. Remove all other USB devices temporarily.
- ► Connect the server to the mains while pushing the ID button on the front panel. Ask a second person to help you if necessary.
- ► Ensure that the Global Error indicator and the ID indicator are flashing to indicate that the server is entering the iRMC recovery state.
- ► Press the Power On / Off button. The system starts the POST process.

  In iRMC recovery mode, the “FUJITSU” logo does not show up.
- ► The system will detect the USB stick.

  If the BIOS cannot identify the USB stick, the pop-up message `Failed to boot for Emergency flash. Please Reset now.` will show up in the center of the screen.
- ► Choose the *Recovery_L* option from the update tool menu to start the iRMC update process.

  CAUTION!

  Do not interrupt the iRMC upgrade process after it has started. If the process is interrupted, the iRMC BIOS may be permanently corrupted.

  If the iRMC does not work after flashing, disconnect the system from the mains and reconnect it again.
- ► Shut down the server by pressing the power On / Off button.
- ► Disconnect the server from the mains to exit the iRMC recovery state.

5.2.2 Verifying system information backup / restore

To avoid the loss of non-default settings when replacing the system board, a backup copy of important system configuration data is automatically stored from the system board NVRAM to the Chassis ID EPROM. After replacing the system board the backup data is restored from the Chassis ID board to the new system board.

In order to verify whether the backup or restore process has been successful, check the System Event Log (SEL) using the ServerView Operations Manager (see also section "Viewing and clearing the System Event Log (SEL)" on page 85).

After replacing the system board

- Check the SEL log files as described in section "Viewing and clearing the System Event Log (SEL)" on page 85 to verify whether the backup data on the Chassis ID EPROM has been restored to the system board:

  ```
  Chassis IDPROM: BMC FW Restore successful
  ```

After replacing the Chassis ID EPROM

In case of the PRIMERGY RX2520 M1 server, the Chassis ID EPROM is integrated on the front panel board.

- Check the SEL log files as described in section "Viewing and clearing the System Event Log (SEL)" on page 85 to verify whether a backup copy of the system board settings has been transferred to the Chassis ID EPROM:

  ```
  Chassis IDPROM: BMC FW Backup successful
  ```

5.2.3 Updating RAID controller firmware

After replacing the RAID controller, it is essential to upgrade the firmware to the latest version. The latest RAID controller firmware version is available from the Fujitsu support web pages at:

http://ts.fujitsu.com/support/ (EMEA market)
http://jp.fujitsu.com/platform/server/primergy/downloads/ (Japanese market)

Fujitsu does not assume responsibility for any damage done to the server or for the loss of any data resulting from firmware updates. For the Japanese market, follow the instructions provided separately.

Using the ServerView Update Manager

For a detailed description on how to update the RAID controller firmware using the ServerView Update Manager or Update Manager Express (UME), please refer to the following manuals:

– ServerView Update Manager:
"ServerView Update Management" user guide

– ServerView Update Manager Express:
"Local System Update for PRIMERGY Servers" user guide

Using the flash tool

The latest firmware files are available as ASPs (Autonomous Support Packages) for Windows or as DOS tools from the Fujitsu support web pages at:

http://ts.fujitsu.com/support/ (EMEA market)
http://jp.fujitsu.com/platform/server/primergy/downloads/ (Japanese market)

- Select *Drivers & Downloads*.
- From the *Select Product* drop down lists, choose your PRIMERGY server or enter its serial or ident number into the search field.
- Select your operating system and version.
- Select the desired component type (e.g. SAS RAID).
- Select your controller from the device list to expand a compilation of available drivers and firmware.
- Select the desired file and click *Download* for further instructions.

5.2.4 Enabling Option ROM scan

In order to configure an expansion card that has been installed or replaced, the card's Option ROM has to be enabled in the system board BIOS. The card's firmware is called by the system BIOS upon reboot and can be entered and configured.

Option ROM can be enabled permanently (e.g. in case of a boot controller that may require frequent setup) or temporarily for one-time configuration. When permanently enabling a controllers's Option ROM, keep in mind that only two Option ROMs can be activated in the system board BIOS at a time.

- ► Enter the BIOS.
- ► From the *Advanced* menu select *Option ROM Configuration*.
- ► Identify the desired PCI slot and set its *Launch Slot # OpROM* setting to *Enabled.*
- ► Save your changes and exit the BIOS.

  Up to two Option ROMs can be activated in the system board BIOS at a time.

  For detailed information on how to access the BIOS and modify settings, refer to corresponding BIOS Setup Utility reference manual.

When the enabled expansion card is initialized during the POST phase of the boot sequence, a key combination is displayed temporarily to enter the expansion card's firmware.

- ► Press the displayed key combination.
- ► Modify the expansion card firmware options as desired.
- ► Save your changes and exit the firmware.

The expansion card's option ROM can now be disabled in the system board BIOS.

Exception: If the expansion card controls a permanent boot device, the card's Option ROM has to remain enabled.

5.2.5 Verifying and configuring the backup software solution

This task only applies to the Japanese market.

Disabling backup drives

Depending on the backup software solution, it may be necessary to disable or delete the backup drive from the backup software drive list and reconfigure backup jobs after completing the maintenance task.

This is the case for the following backup software solutions:

– Netvault for Windows
– ARCServe
– BackupExec

Procedures may differ depending on the backup software. For details, refer to the dedicated documentation provided separately.

Further information on suitable backup software solutions and related documentation is available to Fujitsu service partners from the Fujitsu Extranet pages.

Re-enabling backup drives

If a backup drive has been disabled or deleted from the backup software drive list as described in section 5.1.4 on page 69, it has to be re-enabled to complete the maintenance task.

▶ Re-enable backup drives and revise backup software settings and cronjobs.

Detailed information on suitable backup software solutions and related documentation is available to Fujitsu service partners from the Fujitsu Extranet pages

5.2.6 Resetting the boot retry counter

The boot retry counter is decremented from its preset value every time the POST watchdog initiates a system reboot. When the value has reached ’0’, the system will shut down and power off.

5.2.6.1 Viewing the boot retry counter

The current boot retry counter status is available in the BIOS:

- ► Enter the BIOS.
- ► Select the *Server Mgmt* menu.
- ► Under *Boot Retry Counter* the current number of remaining boot attempts is displayed. The value is further decremented with every failed boot attempt or system reboot resulting from critical system errors.
- ► Exit the BIOS.

5.2.6.2 Resetting the boot retry counter

The boot retry counter should be reset to its original value concluding every service task.

Please note, if the customer does not know about the original boot retry values:

If the system boots up and no further errors occur within 6 hours after that successful boot attempt, the boot retry counter will automatically be reset to its default value. Please take into account, that the specified number of boot attempts can only be determined after this period of time.

If the customer knows about the original boot retry values, proceed as follows to reset or configure the boot retry counter:

Resetting the boot retry counter in the BIOS

- ► Enter the BIOS.
- ► Select the *Server Mgmt* menu.
- ► Under *Boot Retry Counter* press the [+] or [-] keys to specify the maximum number of boot attempts (0 to 7).
- ► Exit the BIOS.

Resetting the boot retry counter using the ServerView Operations Manager

- In the ServerView Operations Manager *Administration* view, select *Server Configuration*.
- If more than one server is managed in SVOM, select the target server and click *Next*.
- From the *Server Configuration* menu pane, choose *Restart Options*.
- Under *Reboot Retries*, specify the maximum number of boot attempts (0 to 7) in the *Default for reboot tries* field.

Resetting the boot retry counter using iRMC web frontend

- Enter the ServerView iRMC web frontend.
- Select the *Server Management* menu.
- The following boot retry counter settings are available under *ASR&R Options:*
  - Under *Retry counter max* specify the maximum number of attempts to boot the operating system (0 to 7).
  - Under *Retry counter* the current number of remaining boot attempts is displayed. Overwrite this value with the maximum number of boot attempts specified above in order to reset the boot retry counter.
- Click *Apply* for the changes to take effect.

For detailed information on iRMC settings, refer to the "Integrated Remote Management Controller" user guide.

5.2.7 Enabling SVOM boot watchdog functionality

If ServerView Operations Manager boot watchdog functionality has been disabled for firmware upgrade purposes (see section 5.1.2 on page 66), it has to be re-enabled to complete the maintenance task.

Timer settings can be configured in the BIOS or using the ServerView iRMC web frontend:

Configuring boot watchdog settings in the BIOS

- ► Enter the BIOS.
- ► Select the *Server Mgmt* menu.
- ► Under *Boot Watchdog* set the *Action* setting to *Reset*.
- ► Save your changes and exit the BIOS.

For detailed information on how to access the BIOS and modify settings, refer to the corresponding BIOS Setup Utility reference manual.

Configuring boot watchdog settings using the iRMC web frontend

- ► Enter the ServerView iRMC web frontend.
- ► Select the *Server Management* menu.
- ► Under *Watchdog Settings* ensure that the check box next to Boot Watchdog is selected. From the drop down list choose *Reset* and specify the desired timeout delay.
- ► Click *Apply* for the changes to take effect.

For detailed information on iRMC settings, refer to the "Integrated Remote Management Controller" user guide.

5.2.8 Enabling replaced components in the system BIOS

When a processor, an expansion card, or a memory module fails, the defective component will be set to *Disabled* or *Failed* in the system BIOS. The server will then reboot with only the intact hardware components remaining in the system configuration. After replacing the defective component, it needs to be re-enabled in the system board BIOS.

- ► Enter the BIOS.

- ► Select the *Advanced* menu.
- ► Select the status menu of the desired component:
  - – Processors: *CPU Status*

    This option is only available for multi-processor systems.
  - – Memory: *Memory Status*
  - – Expansion cards: *PCI Status*
- ► Reset replaced components to *Enable*.
- ► Save your changes and exit the BIOS.

For detailed information on how to access the BIOS and modify settings, refer to the corresponding BIOS Setup Utility reference manual.

5.2.9 Verifying the memory mode

If a memory module fails, the server will reboot and the defective module will be disabled. As a result, the current operation mode (e.g. Mirrored Channel mode) may no longer be available due to a lack of identical memory module pairs. In this case, the operation mode will automatically revert to Independent Channel Mode.

For detailed information on memory operation modes available for your server, refer to section "Memory sequence" on page 197.

After replacing the defective module(s) the memory operation mode is automatically reset to its original state. It is recommended to verify that the operation mode has been correctly.

- ► Enter the BIOS.
- ► Select the *Advanced* menu.
- ► Under *Memory Status* verify that none of the memory modules are marked as *Failed*.
- ► Save your changes (if applicable) and exit the BIOS.

For detailed information on how to access the BIOS and modify settings, refer to the corresponding BIOS Setup Utility reference manual.

5.2.10 Verifying the system time settings

This task only applies to Linux environments.

After the system board has been replaced, the system time is set automatically. By default, the RTC (Real Time Clock) time standard is set as the local time.

If a Linux OS is used and the hardware clock has been configured as UTC (Universal Time, Coordinated) in the operating system, the BMC local time may not be mapped correctly.

- After replacing the system board, ask the system administrator whether the RTC or UTC time standard is to be used as system time.

  If the system time (RTC) is set to UTC, the SEL (System Event Log) time stamps may differ from the local time.

- Enter the BIOS.
- Select the *Main* menu.
- Under *System Time* and *System Date* specify the correct time and date.

  By default, the system time set in the BIOS is RTC (Real Time Clock) local time. If your IT infrastructure relies on universally accepted time standards, set the *System Time* to UTC (Universal Time, Coordinated) instead. Greenwich Mean Time (GMT) can be considered equivalent to UTC.

- Save your changes and exit the BIOS.

For detailed information on how to access the BIOS and modify settings, refer to the corresponding BIOS Setup Utility reference manual

5.2.11 Viewing and clearing the System Event Log (SEL)

5.2.11.1 Viewing the SEL

You can view the System Event Log (SEL) using the ServerView Operations Manager or the ServerView iRMC web frontend:

Viewing the SEL in ServerView Operations Manager

- In ServerView Operations Manager *Single System View* select *Maintenance* from the *Information / Operation* menu.
- Under *Maintenance* select *System Event Log*.
- Select the message type(s) you want to display:
  - Critical events
  - Major events
  - Minor events
  - Informational events

Note on the SVOM Driver Monitor

The *Driver Monitor* view gives you an overview of the monitored components as well as the associated events contained in the system event log on the managed server.

Under *Monitored Components* the monitored components are listed. If a component has the status *Warning* or *Error*, you can select it in the list and click *Acknowledge*. This confirms the event on the server side. You may have to log on to the server beforehand. The status of the component will then be reset to *ok*. To see the new status you must refresh the *Driver Monitor* view with *Refresh*.

For detailed information on how to view and sort the SEL using ServerView Operations Manager, refer to the "ServerView Operations Manager - Server Management" user guide.

Viewing the SEL using the iRMC web frontend

- ► Enter the ServerView iRMC web frontend.
- ► Select the *Event Log* and choose the *Internal Event Log* submenu.
- ► Under *Internal Event Log Content* the SEL is being displayed. In order to filter the list, select the check boxes next to the desired event types and press *Apply* for the changes to take effect.

For detailed information on iRMC settings, refer to the "Integrated Remote Management Controller" user guide.

5.2.11.2 Clearing the SEL

You can clear the System Event Log (SEL) using the ServerView iRMC web frontend:

- ► Enter the ServerView iRMC web frontend.
- ► Select the *Event Log* and choose the *Internal Event Log* submenu.
- ► Under *Internal Event Log Information* click *Clear Internal Event Log* to clear the SEL.

For detailed information on iRMC settings, refer to the "Integrated Remote Management Controller" user guide.

5.2.12 Updating the NIC configuration file in a Linux environment

In order to prevent errors caused by changing network device names (*eth<x>*), it is recommended to store the MAC address (hardware address) of a network interface card in the related NIC configuration file of the Linux OS.

When replacing a network controller or the system board with onboard LAN controllers in a server running Linux OS, the MAC address will change but not automatically be updated in the definition file.

In order to prevent communication problems, it is necessary to update the changed MAC address stored in the related *ifcfg-eth<x>* definition file.

To update the MAC address, proceed as follows:

Procedures may differ depending on your Linux OS or the definition file on the client system. Use the following information as reference. Ask the system administrator to change the definition file.

- After replacing a network controller or the system board, switch on and boot the server as described in section "Switching on the server" on page 64.

  kudzu, the hardware configuration tool for Red Hat Linux, will launch at boot and detect the new and / or changed hardware on your system.

  kudzu may not launch at boot depending on the client's environment.

- Select *Keep Configuration* and *Ignore* to complete the boot process.
- Use the *vi* text editor to specify the MAC address in the HWADDR section of the *ifcfg-eth<x>* file:

  The MAC address can be found on the type label attached to the system board or network controller.

  Example:

  In order to modify the definition file for network controller 1, enter the following command:

  ```
  # vi /etc/sysconfig/network-scripts/ifcfg-eth1
  ```

  In *vi*, specify the new MAC address as follows:

  ```
  HWADDR=xx:xx:xx:xx:xx:xx
  ```

- Save and close the definition file.
- For the changes to take effect, you need to reboot the network by entering the following command:

  ```
  # service network restart
  ```

If the system board or network controller offers multiple LAN ports, it is necessary to update the remaining *ifcfg-eth<x>* definition files accordingly.

- Update the NIC configuration file to reflect the new card sequence and MAC address.

5.2.13 Enabling BitLocker functionality

If BitLocker Drive Encryption has been disabled for maintenance purposes (see section "Disabling BitLocker functionality" on page 65), it has to be re-enabled to complete the service task.

If BitLocker Drive Encryption has been disabled prior to replacing components you won't be asked for a recovery key when rebooting the server after the maintenance task. However, if BitLocker functionality has not been disabled, Windows will enter recovery mode and ask you to input recovery key for further booting.

- ► In this case, ask the system administrator to enter the recovery key in order to boot the operating system.

- ► Ask the system administrator to enable BitLocker-protection on the operating system drive, using the BitLocker setup wizard available either from the Control Panel or Windows Explorer.
  - ► Open Bitlocker Drive Encryption by clicking the *Start* button, clicking *Control Panel*, clicking *Security*, and then clicking *Bitlocker Drive Encryption*.

    Administrator permission required: If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
  - ► To enable a temporarily disabled BitLocker, click *Turn On BitLocker*.
  - ► Follow the instructions in the BitLocker Setup wizard.

For further information on how to enable BitLocker drive encryption, please refer to the Microsoft Knowledge Base.

Fujitsu service partners will find additional information (also available in Japanese) on the Fujitsu Extranet web pages.

5.2.14 Performing a RAID array rebuild

After replacing a hard disk drive that has been combined into a RAID array, RAID rebuild will be performed completely unattended as a background process.

- ► Ensure that the RAID array rebuild has started normally. Wait until the progress bar has reached at least one percent.
- ► Inform the customer about the remaining rebuild time, based on the displayed duration estimate.

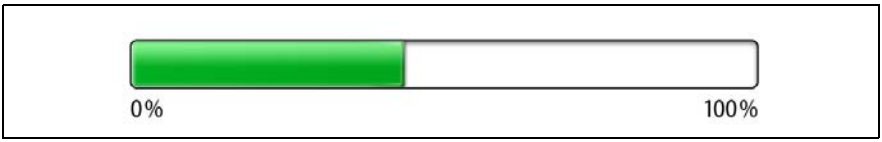


Figure 13: Progress bar (RAID array rebuild)

CAUTION!

The system is now operational, however, data redundancy will not be available until the RAID array rebuild is complete. Depending on the hard disk drive capacity the overall process can take up to several hours, in some cases even days.

You may notice a slight performance impact during rebuild.

5.2.15 Looking up changed MAC / WWN addresses

When replacing a network controller, the MAC (Media Access Control) and WWN (World Wide Name) addresses will change.

In addition to the procedures described below, MAC / WWN addresses can also be found on the type label attached to a network controller or system board.

5.2.15.1 Looking up MAC addresses

- ► Enter the ServerView iRMC web frontend.
- ► Select the *System Information* menu.

- Under *Network Inventory*, you will find detailed information on each network controller in the managed PRIMERGY server, including its MAC address.

  This information is only available with the iRMC S4 or above.

  Only network controllers supporting the Command Line Protocol (CLP) will be displayed.

- Inform the customer about the changed MAC address.

5.2.15.2 Looking up WWN addresses

Emulex FC / FCoE adapters

- Enable the network controller's Option ROM in the system board BIOS as described in section "Enabling Option ROM scan" on page 78.
- Restart the server.
- During boot, as soon as the Emulex BIOS utility option appears, press ALT + E or CTRL + E.
- Under *Emulex Adapters in the System* you will find all available Emulex adapters and their WWN addresses.
- Note down the new 16-digit WWN address.
- Press Esc to exit the Emulex BIOS utility.
- Inform the customer about the changed WWN address.

QLogic FC adapters

- Enable the network controller's Option ROM in the system board BIOS as described in section "Enabling Option ROM scan" on page 78.
- Restart the server.
- During boot, as soon as the QLogic BIOS utility option appears, press ALT + Q or CTRL + Q.
- Under *Select Host Adapter* use the arrow keys ↑/↓ to select the desired FC / FCoE adapter and press Enter.
- From the *Fast!UTIL Options* menu, select *Configuration Settings*, and press Enter.
- From the *Configuration Settings* menu, select *Adapter Settings*, and press Enter.

- ► Note down the new 16-digit WWN address found under *Adapter Port Name*.
- ► Press Esc to return to the main menu and exit the QLogic BIOS utility.
- ► Inform the customer about the changed WWN address.

5.2.16 Using the Chassis ID Prom Tool

The Chassis ID EPROM located on a dedicated Chassis ID board or on your server's front panel board contains system information like server name and model, housing type, serial number and manufacturing data.

In order to integrate your system into the ServerView management environment and to enable server installation using the ServerView Installation Manager, system data needs to be complete and correct.

After replacing the Chassis ID EPROM, system information has to be entered using the Chassis ID Prom tool. The tool and further instructions are available to maintenance personnel from the Fujitsu Technology Solutions Extranet:

https://partners.ts.fujitsu.com/com/service/ps/Servers/PRIMERGY/

- ► Select your PRIMERGY system from the main area of the page.
- ► From the categories selection, choose *Software & Tools Documentation*.
- ► In the *Tools* area click *Tools: Chassis-IDProm Tool* to download the file (*tool-chassis-Idprom-Tool.zip*).

For the Japanese market, follow the instructions provided separately.

Note on Cool-safe® Advanced Thermal Design (ATD)

If the Cool-safe® Advanced Thermal Design (ATD) option is available and has been enabled for your server, please set information within the Chassis ID Prom Tool accordingly.

The ATD option can only be ordered from the manufacturer as a factory preset. To find out if your server is ATD-enabled, check for the ATD logo on the identification rating plate.

For further information on Cool-safe® Advanced Thermal Design (ATD), please refer to your server's operating manual.

CAUTION!

Please note that you can only set the ATD flag. Resetting the ATD flag using the Chassis ID Prom Tool is not possible!

5.2.17 Configuring LAN teaming

Use ServerView Operations Manager to obtain detailed information on existing LAN teams:

- In ServerView Operations Manager *Single System View* select *System Status* from the *Information / Operation* menu.
- Under *Network Interfaces* select *LAN Teaming*.
- The *Network Interfaces (Summary)* overview shows all configured LAN teams and their components. Choose a LAN team to display further details:
  - *LAN Team Properties*: Properties of the selected LAN team
  - *LAN Team Statistics*: Available statistics about the selected LAN team

For more detailed information, refer to the "ServerView Operations Manager - Server Management" user guide.

5.2.17.1 After replacing / upgrading LAN controllers

Please note when re-using a replaced LAN controller:

- Confirm with the customer whether the LAN controller you have replaced has been used as part of a LAN teaming configuration.
- If LAN teaming has been active, you will need to restore the configuration using the LAN driver utility after replacing the LAN controller.

  Ensure that the controllers have been assigned as primary or secondary according to your requirements.

For details, refer to the relevant LAN driver manual.

5.2.17.2 After replacing the system board

- Confirm with the customer whether the onboard LAN controller you have replaced has been used as part of a LAN teaming configuration.

- If LAN teaming has been active, you will need to restore the configuration using the LAN driver utility after replacing the system board.

For details, refer to the relevant LAN driver manual.

5.2.18 Switching off the ID indicator

Press the ID button on the front panel, or use the iRMC web frontend or ServerView Operations Manager to switch off the ID indicator after the maintenance task has been concluded successfully.

For further information, refer to section "Locating the defective server" on page 47 or to the "ServerView Suite Local Service Concept (LSC)" and "Integrated Remote Management Controller" user guides.

Using the ID button on the front panel

- Press the ID button on the front panel to switch off the ID indicators.

Using the iRMC web frontend

- Enter the ServerView iRMC web frontend.
- Under *System Overview*, click *Identify LED Off* to switch off the ID indicators.

Using ServerView Operations Manager

- In ServerView Operations Manager *Single System View* and press the *Locate* button in the title bar to switch off the ID indicator.

5.2.19 Performing a fan test after replacing a defective fan

After replacing a defective system fan or power supply unit containing a defective fan, the fan error indicators will stay lit until the next fan test. By default, a fan test is automatically started every 24 hours. The first automatic fan test being performed after replacing a fan will turn off the fan error indicator.

If you want to start the fan test manually, you can do so by following the description below:

Executing the fan test via the iRMC Web interface

- ► Log into the iRMC web interface.
- ► Under *Sensors* select *Fans*.
- ► Select the replaced fan in the system fans group and click *Start Fan Test*.

i For detailed information on iRMC settings, refer to the "Integrated Remote Management Controller" user guide.

Executing the fan test via ServerView Operations Manager

- ► Open the ServerView Operations Manager and log in.
- ► Under *Administration* select *Server Configuration*.
- ► In the hierarchy tree of the *Server list* tab, select the server to be configured.
- ► In the right-hand side of the window, specify the details on the selected server and confirm your entries by clicking *GO...*.

  In the left-hand section of the window, the *Configuration* tab is being activated.
- ► In the navigation area of the *Configuration* tab, select *Other Settings*.
- ► Under *Daily Fan Test*, set the daily fan test time to a few minutes from the current time. (Ensure to note down your previous setting.)
- ► Click *Save Page*.
  The fan test will be started at the specified time.
- ► After the fan test is complete, restore the time setting to its initial value and click *Save Page*.

i For more detailed information, refer to the "ServerView Operations Manager" user guide.

For the Japanese market: Executing the fan test via Chassis ID Prom Tool

i Please follow the instructions provided separately.

6 Power supply units

Safety notes

CAUTION!

- Do not disassemble the power supply unit. Doing so may cause electric shock.
- Areas around the power supply unit may remain extremely hot after shutdown. After shutting down the server, wait for hot components to cool down before removing the power supply unit.
- When installing a power supply unit, ensure that the connector of the power supply unit is not damaged or bent.
- If the power supply unit is hard to remove, do not pull it out by force.
- The power supply unit is heavy, so handle it carefully. If you drop it by mistake, injuries may result.
- For further safety information, please refer to chapter "Important information" on page 35.

6.1 Basic information

The PRIMERGY RX2520 M1 server can be equipped:

– with up to two power supply units that automatically adjust to any mains voltage in the range of 100 VAC to 240 VAC

Power redundancy is possible with two power supply units . The effective power of the power supply units may not differ.

CAUTION!

The server supports a mains voltage in the range of 100 VAC to 240 VAC. You may only operate the server if its rated voltage range corresponds to the local mains voltage.

6.1.1 Power supply unit configurations

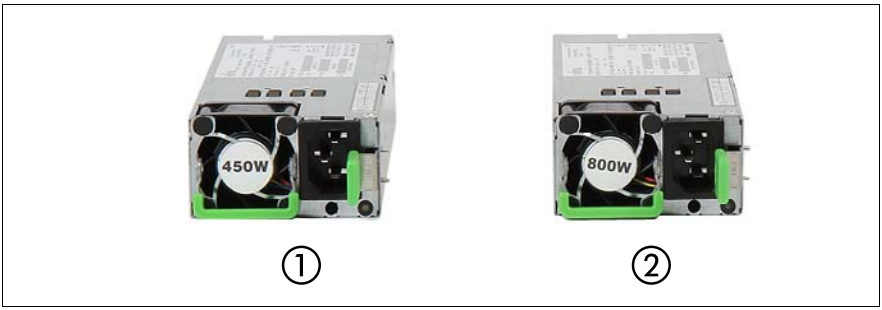


Figure 14: Hot-plug power supply units: 450 W AC (1), 800 W AC (2),

All different hot-plug power supply units are to install, to remove or to replace in the same way.

6.1.2 Assembly rules

– Mixed assembly of 450 W and 800 W hot-plug power supply units is not supported.

– Always install a dummy cover into an unused power supply unit bay to comply with applicable EMC regulations and satisfy cooling requirements.

– For a redundant power supply you need two hot-plug power supply units.

Note for servers using CMA (Cable Management Arm)

Regarding of removing power supply units, additional tasks are needed, due to an interference between CMA stopper and the power supply units.

- ► Unlock the CMA stopper.
- ► Remove the CMA stopper with the mounted crossbar.
- ► Support the CMA stopper, the crossbar and the CMA including cables with your right hand.
- ► Remove the power supply unit and install a dummy cover into the empty bay.
- ► Remount the complete assembly (CMA stopper, crossbar and CMA) into the rail.

6.1.3 Power supply unit slots

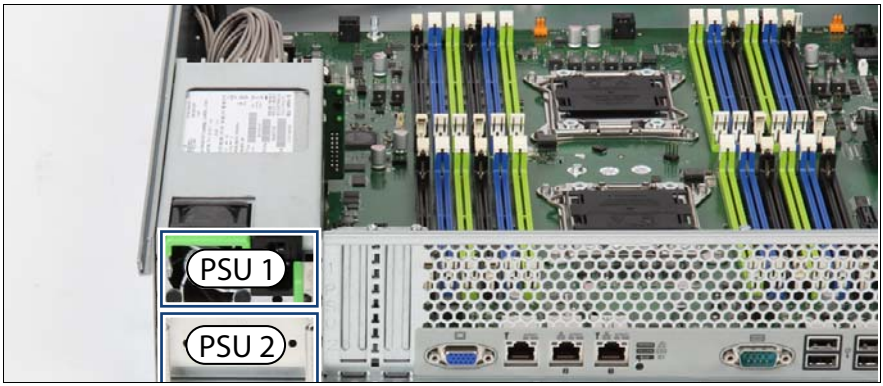


Figure 15: Power supply unit slots

6.2 Installing hot-plug power supply units

Customer Replaceable Unit (CRU)

Hardware: 5 minutes

Tools:	tool-less

6.2.1 Preliminary steps

No steps needed.

6.2.2 Removing the dummy cover

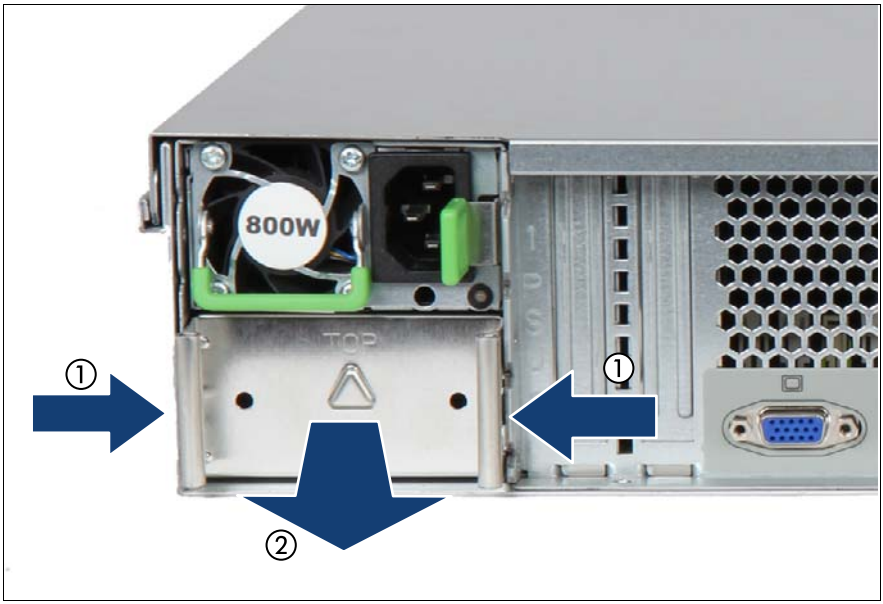


Figure 16: Removing the dummy cover

► Press in on both release latches (1) and remove the dummy cover (2).

CAUTION!

Keep the dummy cover for future use. If a power supply unit is removed and not immediately replaced by a new one, a dummy cover must be replaced in the slot to comply with applicable EMC regulations and satisfy cooling requirements.

6.2.3 Installing a hot-plug power supply unit

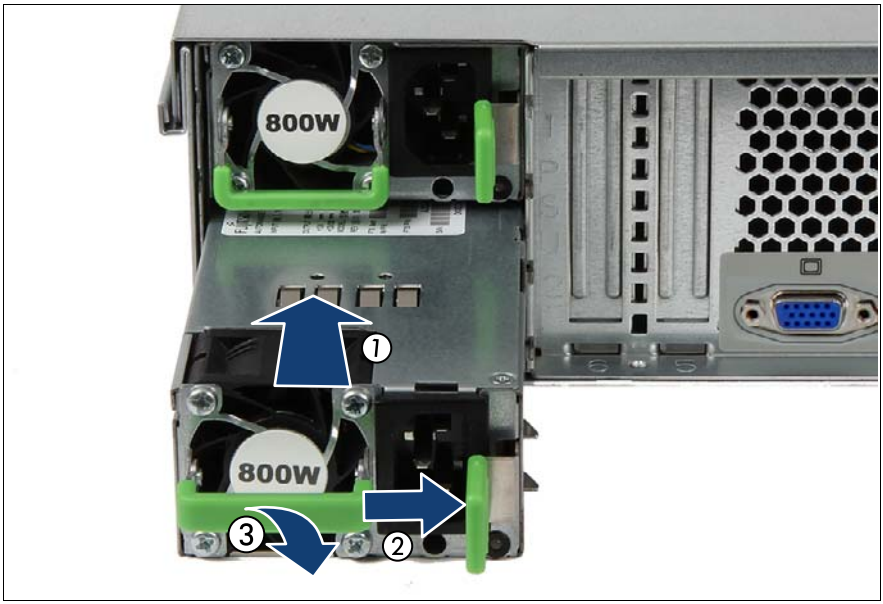


Figure 17: Installing the hot-plug power supply unit

- Push the power supply unit into its bay (1) as far as it will go until the release latch snaps in place (2).
- Fold down the handle on the power supply unit(3).

CAUTION!

Ensure that the power supply unit properly engages in its bay and is locked in position in order to prevent it from sliding out of the chassis during transportation.

6.2.4 Concluding steps

- "Connecting the server to the power source" on page 62

6.3 Removing a hot-plug power supply unit

Customer Replaceable Unit (CRU)

Hardware: 5 minutes

Tools:	tool-less

Note for servers using CMA (Cable Management Arm)

Regarding of removing power supply units, additional tasks are needed, due to an interference between CMA stopper and the power supply units.

- ► Unlock the CMA stopper.
- ► Remove the CMA stopper with the mounted crossbar.
- ► Support the CMA stopper, the crossbar and the CMA including cables with your right hand.
- ► Remove the power supply unit and install a dummy cover into the empty bay.
- ► Remount the complete assembly (CMA stopper, crossbar and CMA) into the rail.

6.3.1 Preliminary steps

- ► "Locating the defective server" on page 47
- ► Remove the power cord from the dedicated power supply unit as described in section "Disconnecting power cords" on page 50

6.3.2 Removing a hot-plug power supply unit

Figure 18: Removing the hot-plug power supply unit

- ► Push the handle of the power supply unit halfway upward in the direction of the arrow (1).
- ► Push the green release latch in direction of the arrow (2).
- ► While keeping the green release latch pressed, pull the power supply unit out of its slot (3).

CAUTION!

Never leave the bay for the power supply unit empty for more than two minutes during operation. Otherwise, excessive temperatures could damage system components.

6.3.3 Installing a dummy cover

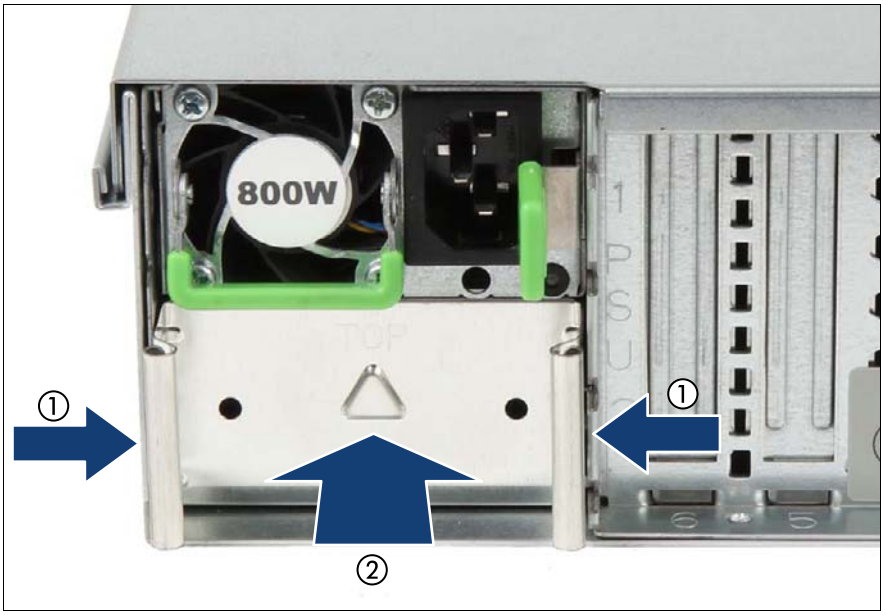


Figure 19: Installing a dummy cover

- Insert the dummy cover into the empty bay with the impressed arrow symbol facing up.
- Press in on both release latches on the dummy cover (1) and carefully insert the dummy cover into its bay (2) until it locks in place.

CAUTION!

Always install dummy covers into unused bay ts to comply with applicable EMC regulations and satisfy cooling requirements.

6.3.4 Concluding steps

- "Connecting the server to the power source" on page 62

6.4 Replacing a hot-plug power supply unit

Customer Replaceable Unit (CRU)

Hardware: 5 minutes

Tools: tool-less

CAUTION!

- When replacing a power supply unit in a non-redundant power supply configuration, the server must be switched off first.
- Replace the power supply unit after specifying the one that breaks down at work by revitalization.
- Ensure to replace a defective power supply unit by a new unit of the same type.

6.4.1 Preliminary steps

- ► "Locating the defective server" on page 47
- ► "Locating the defective component" on page 49
- ► In non-redundant power supply configurations, shut down the server as described in section "Shutting down the server" on page 49.
- ► "Disconnecting power cords" on page 50

6.4.2 Removing the defective hot-plug power supply unit

- ► Remove the defective power supply unit as described in section "Removing a hot-plug power supply unit" on page 101.

6.4.3 Installing the new hot-plug power supply unit

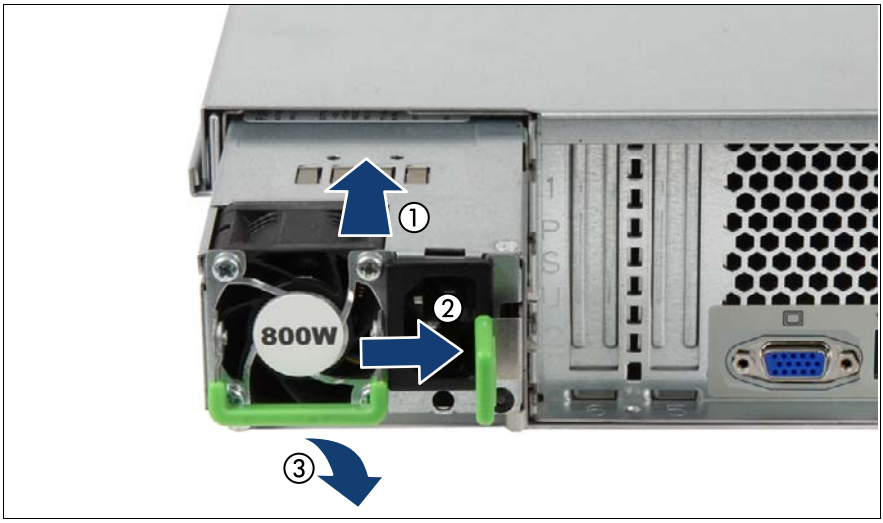


Figure 20: Installing the hot-plug power supply unit

- Insert the power supply unit into its slot.
- Push the power supply unit into its slot (1) as far as it will go until the locking latch snaps in place (2).

  CAUTION!

  Ensure that the power supply unit properly engages in its slot and is locked in position in order to prevent it from sliding out of the chassis during transportation.

- If applicable, fold down the handle on the power supply unit(3).

6.4.4 Concluding steps

- "Connecting the server to the power source" on page 62
- In non-redundant PSU configurations, swich on the server as described in section "Switching on the server" on page 64
- "Performing a fan test after replacing a defective fan" on page 93

6.5 Upgrading a power supply from 450 W to 800 W

Basic information

CAUTION!

No mixed power supply configuration is allowed.

Customer Replaceable Unit (CRU)

Hardware: 5 minutes

Tools: tool-less

6.5.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- In non-redundant power supplyconfigurations, shut down the server as described in section "Shutting down the server" on page 49.
- "Disconnecting power cords" on page 50

6.5.2 Removing the hot-plug power supply unit

CAUTION!

If you want to upgrade the power supply unit from 450W to 800 W hot-plug the running of the mixed configuration must not exceed 5 minutes.

- "Removing a hot-plug power supply unit" on page 101

6.5.3 Installing the new hot-plug power supply unit

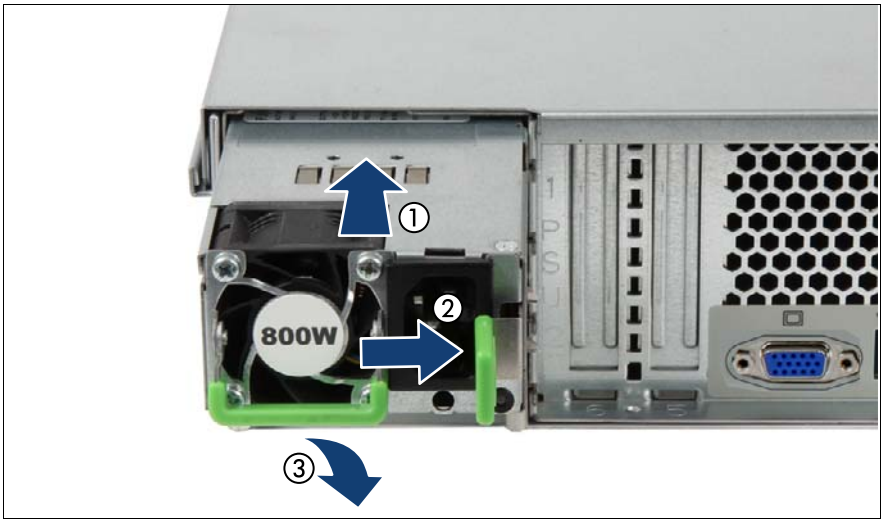


Figure 21: Installing the hot-plug power supply unit

- ► Insert the power supply unit into its bay.
- ► Push the power supply unit into its bay (1) as far as it will go until the release latch snaps in place (2).

  When upgrading redundant power supply configurations from 450 W to 800 W power supply unit, please note the following:

  After replacing the first power supply unit, the CSS indicator will start flashing (entry into SEL), indicating an unsupported mixture of power supply units with different power output.

  The CSS indicator LED will stop flashing as soon as the second power supply unit has been replaced as well.

  CAUTION!

  Ensure that the power supply unit properly engages in its slot and is locked in position in order to prevent it from sliding out of the chassis during transportation.

- ► If applicable, fold down the handle on the power supply unit(3).

6.5.4 Concluding steps

- "Connecting the server to the power source" on page 62
- "Enabling BitLocker functionality" on page 88

6.6 Replacing the power backplane

Field Replaceable Unit (FRU)

Hardware: 10 minutes

Tools: tool-less

6.6.1 Preliminary steps

- "Locating the defective server" on page 47
- "Disabling BitLocker functionality" on page 65
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51
- "Removing the housing cover" on page 55
- "Removing the air duct" on page 56

6.6.2 Disconnecting cables

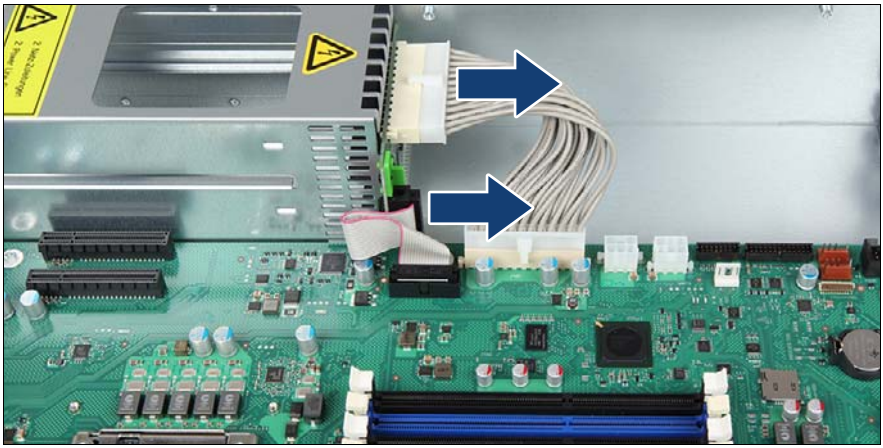


Figure 22: Disconnecting cables from the power backplane

► Remove the cables from the power backplane.

6.6.3 Removing the power backplane

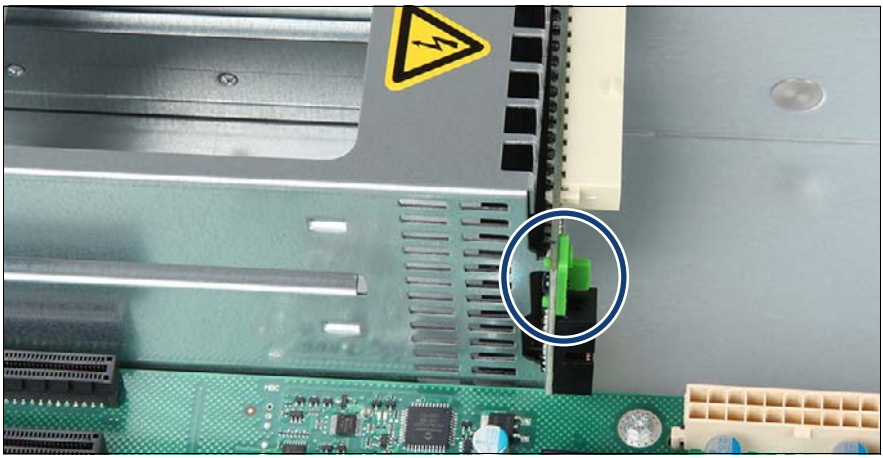


Figure 23: Removing the power backplane (A)

► Unlock the locking mechanism of the power backplane.

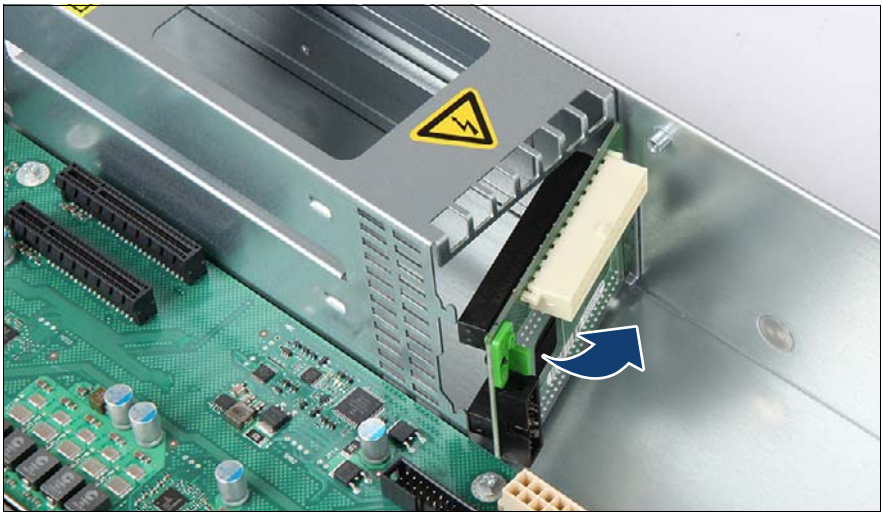


Figure 24: Removing the power backplane (B)

- ► Fold the power backplane in the direction of the arrow.
- ► Push the power backplane upward.
- ► Remove the power backplane.

6.6.4 Installing the power backplane

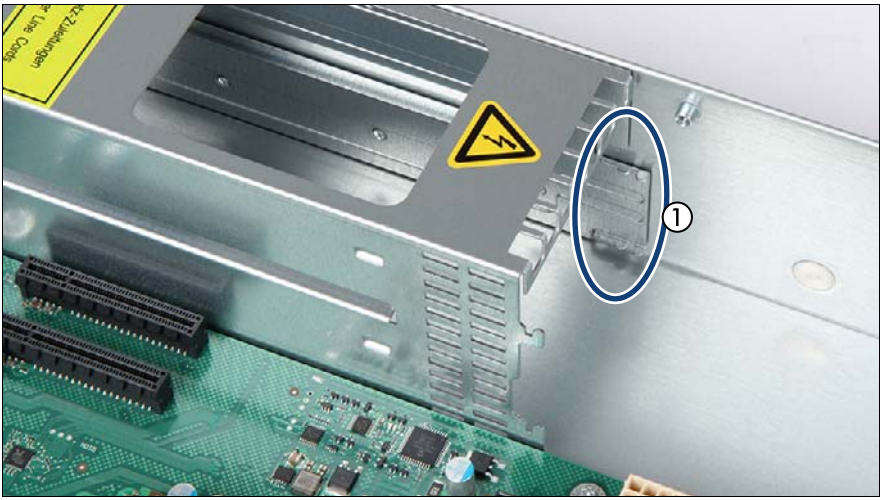


Figure 25: Installing the power backplane (A)

► Insert the new power backplane into the guiding hooks of the chassis (1).

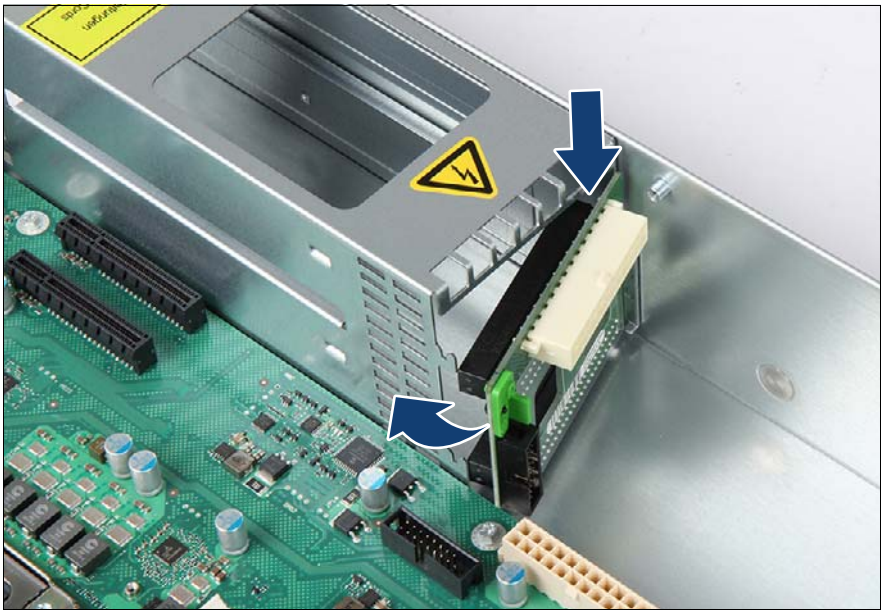


Figure 26: Installing the power backplane (B)

► Slide the power backplane downward in the guiding hooks.

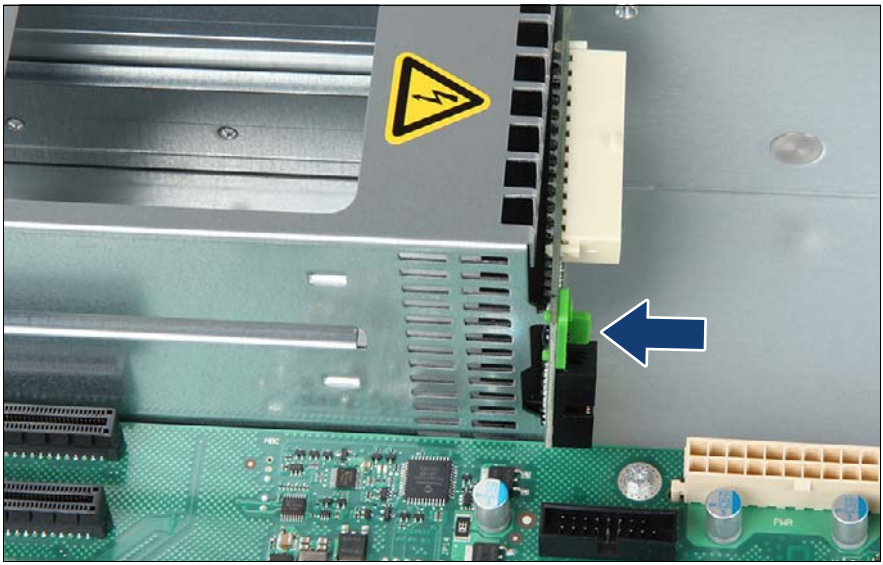


Figure 27: Locking the power backplane

► Press the power backplane in the direction of the arrow to lock it.

6.6.5 Reconnecting cables

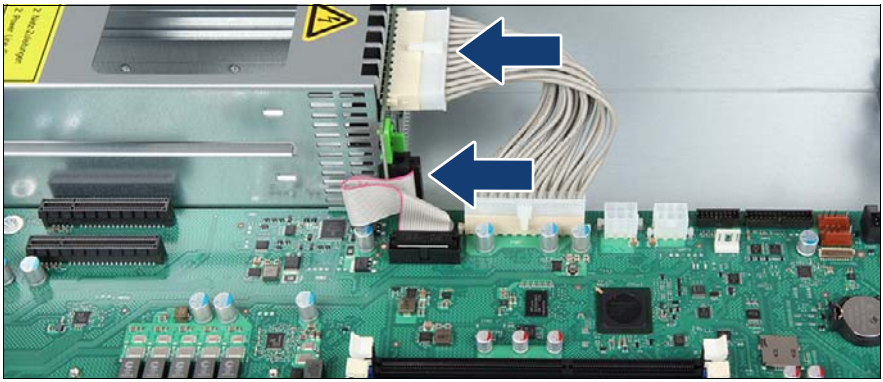


Figure 28: Connecting cables

► Connect the cables.

6.6.6 Concluding steps

- "Installing the air duct" on page 57
- "Mounting the housing cover" on page 59
- "Sliding the server into the rack" on page 62

  If the server has been completely removed from the rack for maintenance purposes, reinstall and secure it in the rack as described in section "Mounting the server in the rack" on page 59.
- "Connecting the server to the power source" on page 62
- "Enabling BitLocker functionality" on page 88

7 Hard disk drives / solid state drives

Safety notes

CAUTION!

- The hard disk drive must not be removed from the installation frame by anyone except a service technician.
- HDD / SSD modules must all be marked clearly so that they can be reinstalled into their original mounting locations after an upgrade. Otherwise, data may be lost.
- Do not touch the circuitry on boards or soldered parts. Hold the metallic areas or the edges of the circuit boards.
- Before removing a hard disk drive, wait for about 30 seconds until the disk has stopped spinning completely.
- When a hard disk drive is starting up, a resonant noise may be audible for a short while. This does not indicate a failure.
- Depending on the OS, you can configure the write cache settings for the hard disk drives. If a power failure should occur while the write cache is enabled, cached data may be lost.
- When disposing of, transferring, or returning a hard disk or solid state drive, wipe out the data on the drive for your own security.
- Rough handling of hard disk drives may damage the stored data. To cope with any unexpected problems, always back up important data. When backing up data to another hard disk drive, you should make backups on a file or partition basis.
- Handle the device on a shock and vibration free surface.
- Do not use the device in extremely hot or cold locations, or locations with extreme temperature changes.
- Never attempt to disassemble a hard disk or solid state drive.
- For further safety information, please refer to chapter "Important information" on page 35.

7.1 Basic procedures

– Solid state drives (SSDs) are always equipped before installing hard disk drives.

– Hard disk drives / solid state drives with different capacities are installed from highest to lowest capacity.

– Hard disk drives with different rotation speeds are installed from highest to lowest speed.

– When installing hard disk drives with different bus technologies (SAS or SATA), first install SAS drives and then SATA drives.

– Please refer to sections "Mounting order for 2.5-inch HDDs / SSDs" on page 116 for a complete overview of the mounting sequence.

– Install dummy modules into unused HDD / SSD bays.

The mounting order described above is only relevant for the factory manufacturing process. In case of upgrading a system you need not consider this mounting sequence.

7.2 2.5-inch HDD / SSD configurations

7.2.1 Mounting order for 2.5-inch HDDs / SSDs

Maximum configuration: 16x 2.5-inch HDDs / SSDs

Basic information

– Solid state drives (SSDs) are always equipped before installing hard disk drives.

– If only one HDD/SSD module is installed, the HDD/SSD module will be installed in position 1. Empty bays must be equipped with a dummy module.

7.2.1.1 HDD / SSD mounting order for 4x 2.5-inch HDD / SSD configuration

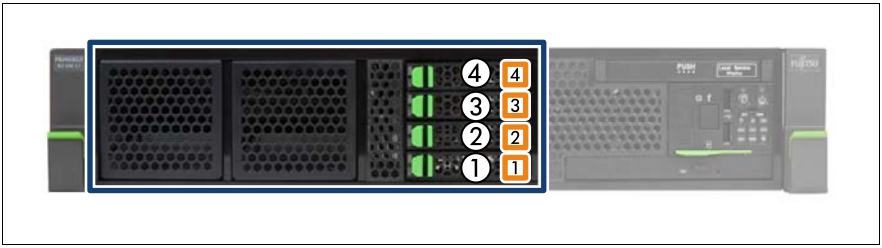


Figure 29: 2.5-inch HDD / SSD mounting order configuration 2 and 3

◯	Mounting order
□	Bay number

7.2.1.2 HDD / SSD naming scheme for 4x 2.5-inch HDD / SSD configuration

The HDD / SSD numbering as listed in the ServerView RAID Manager differs from the HDD mounting order:

2.5-inch HDDs / SSDs		
HDD	**RAID Manager #**	**Channel**
1	0	1
2	1	1
3	2	1
4	3	1

Table 4: HDD naming scheme

7.2.1.3 HDD / SSD mounting order for 8x 2.5-inch HDD / SSD configurations

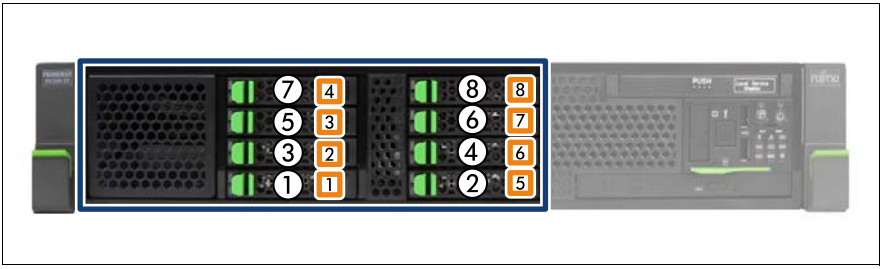


Figure 30: 2.5-inch HDD / SSD mounting order configuration 4

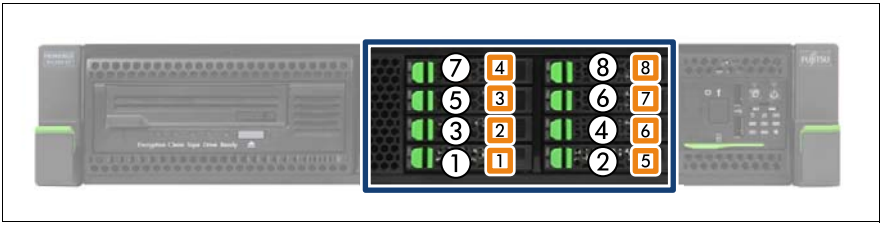


Figure 31: 2.5-inch HDD / SSD mounting order configuration 6

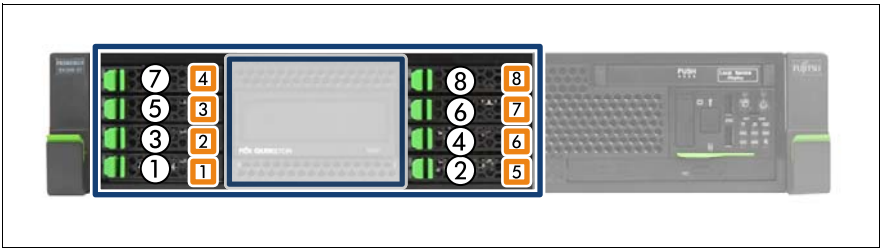


Figure 32: 2.5-inch HDD / SSD mounting order configuration 5

◯	Mounting order
□	Bay number

7.2.1.4 HDD / SSD naming scheme for 8x 2.5-inch HDD / SSD configurations

The HDD / SSD numbering as listed in the ServerView RAID Manager differs from the HDD mounting order:

2.5-inch HDDs / SSDs					
HDD	**RAID Manager #**	**Channel**	**HDD**	**RAID Manager #**	**Channel**
1	0	1	2	4	2
3	1	1	4	5	2
5	2	1	6	6	2
7	3	1	8	7	2

Table 5: HDD naming scheme

7.2.1.5 HDD / SSD mounting order for 12x 2.5-inch HDD / SSD configuration

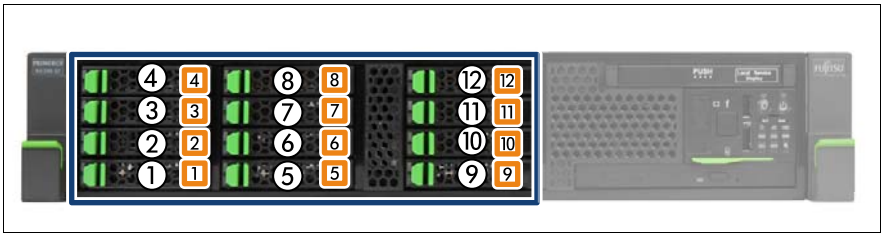


Figure 33: 2.5-inch HDD / SSD mounting order configuration 7

◯	Mounting order
□	Bay number

7.2.1.6 HDD / SSD naming scheme for 12x 2.5-inch HDD / SSD configuration

The HDD / SSD numbering as listed in the ServerView RAID Manager differs from the HDD mounting order:

2.5-inch HDDs / SSDs	
HDD	**RAID Manager #**
1	0
2	1
3	2
4	3
5	4
6	5
7	6
8	7
9	8
10	9
11	10
12	11

Table 6: HDD naming scheme

7.2.1.7 HDD / SSD mounting order for 16x 2.5-inch HDD / SSD configuration

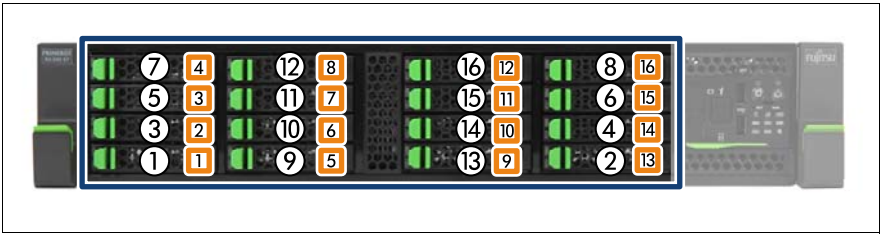


Figure 34: 2.5-inch HDD / SSD mounting order configuration 8

◯	Mounting order
□	Bay number

7.2.1.8 HDD / SSD naming scheme 16x 2.5-inch HDD / SSD configuration

The HDD / SSD numbering as listed in the ServerView RAID Manager differs from the HDD mounting order:

2.5-inch HDDs / SSDs	
HDD	**RAID Manager #**
1	0
2	12
3	1
4	13
5	2
6	14
7	3
8	15
9	4
10	5
11	6
12	7
13	8
14	9
15	10
16	11

Table 7: HDD naming scheme

7.2.2 Installing 2.5-inch HDD / SSD modules

Customer Replaceable Unit (CRU)

Hardware: 5 minutes

Tools: tool-less

7.2.2.1 Preliminary steps

► Locate the correct drive bay as described in section "Mounting order for 2.5-inch HDDs / SSDs" on page 116.

7.2.2.2 Removing a 2.5-inch dummy module

Figure 35: Removing a 2.5-inch dummy module

► Press both tabs together (1) and pull the dummy module out of its bay (2).

CAUTION!

Save the dummy module for future use.
Always replace dummy modules into unused HDD / SSD bays to comply with applicable EMC regulations and satisfy cooling requirements.

7.2.2.3 Installing a 2.5-inch HDD / SSD module

Figure 36: Opening the 2.5-inch HDD / SSD module locking lever

► Pinch the green locking clips (1) and open the locking lever (2).

Figure 37: Inserting the 2.5-inch HDD / SSD module

- ► Insert the HDD module into a drive bay and carefully push back as far as it will go (1).
- ► Close the locking lever to lock the hard disk drive in place (2).

7.2.2.4 Concluding steps

- ► "Performing a RAID array rebuild" on page 89

7.2.3 Removing 2.5-inch HDD / SSD modules

Customer Replaceable Unit (CRU)

Hardware: 5 minutes

Tools: tool-less

7.2.3.1 Preliminary steps

- ► If the HDD / SSD module to be removed is combined into a RAID array, please proceed as follows:

RAID level	Procedure
RAID 0	Only remove an HDD module combined in a RAID 0 array if defective. **CAUTION!** Removing an operational HDD module will result in data loss!
RAID 1 RAID 5	Removing an HDD module from a RAID 1 or RAID 5 array will not result in data loss. However, the removed drive needs to be replaced immediately by an HDD module of the same or larger capacity. After replacing the HDD module, RAID rebuild will be performed as a background process as described in section "Performing a RAID array rebuild" on page 89.

In order to permanently remove an operational HDD module that is part of a RAID array from the server, you first need to delete the array using ServerView RAID Manager or BIOS Utility.

CAUTION!

All data on all HDDs / SSDs in the array will be lost! Be sure to back up your data before deleting a RAID array.

For further information, please refer to the "ServerView Suite RAID Management" user guide and manuals of RAID controller.

7.2.3.2 Removing a 2.5-inch HDD / SSD module

Figure 38: Disconnecting a 2.5-inch HDD / SSD module

- Pinch the green locking clips (1) and fully open the locking lever (2).

  Thereby, the HDD / SSD module is pushed out of its drive bay by about 1 cm and disconnected from the SAS / SATA backplane.

- Wait about 30 seconds to allow the hard disk drive to spin down.

  This is not necessary when removing a solid state drive.

Figure 39: Removing a 2.5-inch HDD / SSD module

► Pull the HDD / SSD module completely out of its bay.

7.2.3.3 Installing a 2.5-inch dummy module

CAUTION!

If the removed HDD / SSD module is not replaced immediately, always replace a dummy module into the unused HDD / SSD bay to comply with applicable EMC regulations and satisfy cooling requirements.

Figure 40: Installing a 2.5-inch dummy module

► Slide the dummy module into the drive bay until it locks in place.

7.2.3.4 Concluding steps

► "Performing a RAID array rebuild" on page 89

7.2.4 Replacing a 2.5-inch HDD / SSD module

Customer Replaceable Unit (CRU) **Hardware: 5 minutes**

Tools: tool-less

CAUTION!

- Only remove an HDD / SSD module during operation if the drive is not currently being accessed. Observe the indicators for the corresponding HDD / SSD modules, see operating manual of your server.

- Under no circumstances should you remove an HDD / SSD module while the system is in operation if you are not sure that the drive is operated by a RAID controller and belongs to a disk array that is operating in RAID level 0, 1, 1E, 10, 5, 50, 6 or 60.

  An HDD / SSD module can only be replaced during operation in conjunction with a corresponding RAID configuration.

- All HDD / SSD modules (drives) must be uniquely identified so that they can be reinstalled in their original mounting locations later. If this is not done, existing data can be lost.

7.2.4.1 Preliminary steps

► "Locating the defective server" on page 47

► Locate the defective HDD / SSD module as described in section "Local diagnostic indicators on the front" on page 49.

Only applicable for removing intact HDD / SSD modules:

► Before removing a non-defective HDD / SSD module, put the drive into "Offline" mode using your RAID configuration software.

7.2.4.2 Removing a 2.5-inch HDD / SSD module

► Remove the HDD / SSD module to be replaced from the server as described in section "Removing a 2.5-inch HDD / SSD module" on page 125.

7.2.4.3 Installing a 2.5-inch HDD / SSD module

► Install the new HDD / SSD module into the empty drive bay as described in section "Installing 2.5-inch HDD / SSD modules" on page 121

7.2.4.4 Concluding steps

► "Performing a RAID array rebuild" on page 89

7.3 Replacing SAS / SATA HDD / SSD backplanes

7.3.1 Replacing the 4x 2.5-inch HDD SAS backplane

Field Replaceable Unit (FRU)

Hardware: 10 minutes

Tools:	Phillips PH2 / (+) No. 2 screw driver

7.3.1.1 Preliminary steps

- "Locating the defective server" on page 47
- "Disabling BitLocker functionality" on page 65
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- Remove all HDD / SSD modules from the server as described in section "Removing 2.5-inch HDD / SSD modules" on page 124.

  CAUTION!

  Ensure that all hard disk drives are uniquely identified so that you can reinsert them into their original bays after replacing the HDD backplane.

- "Getting access to the component" on page 51
- "Removing the fan box" on page 144

7.3.1.2 Removing the 4x 2.5-inch SAS HDD backplane

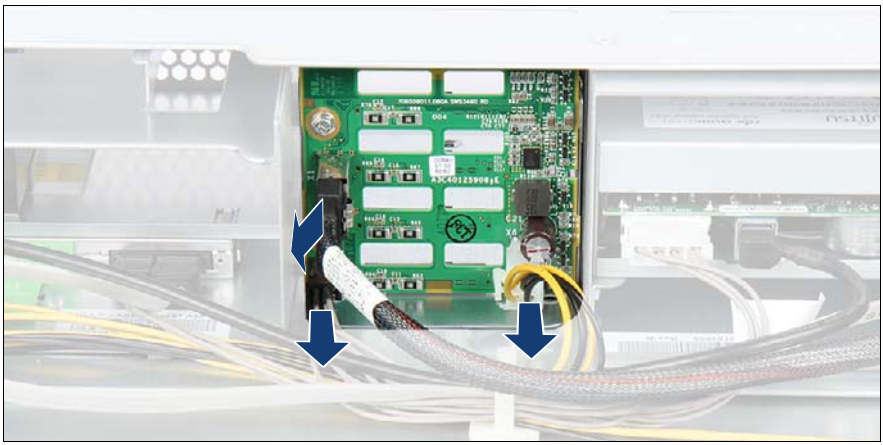


Figure 41: Disconnecting cables from the 4x 2.5-inch HDD SAS backplane

- ► Disconnect all cables from the 4x 2.5-inch HDD SAS backplane:
  - – SAS / SATA cable
  - – Power cables

Figure 42: Removing the 4x 2.5-inch HDD SAS backplane

- ► Remove the screw.
- ► Remove the 4x 2.5-inch HDD SAS backplane.

7.3.1.3 Installing the 4x 2.5-inch HDD SAS backplane

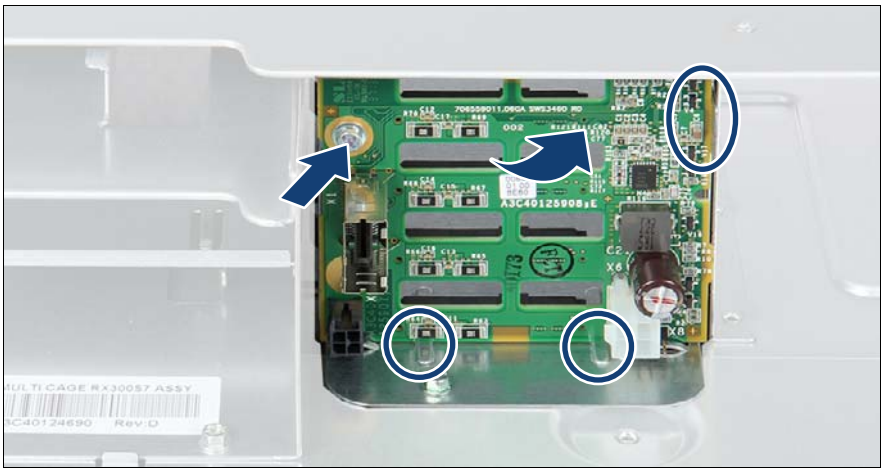


Figure 43: Installing the 2.5-inch HDD SAS backplane

- ► Insert the 4x 2.5-inch HDD SAS backplane in that way that it is in the guiding recesses (see circles).
- ► Fasten the 4x2.5-inch HDD SAS backplane with the screw (see arrow).

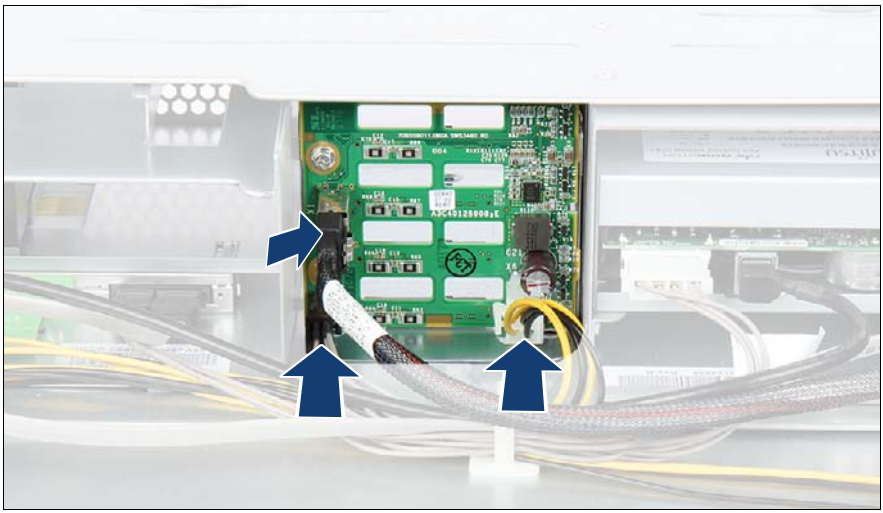


Figure 44: Reconnecting cables to the 4x 2.5-inch HDD SAS backplane

- Reconnect all cables to the 2.5-inch HDD SAS backplane:
  - Power cable C4 to SAS backplane connector X6
  - If applicable power cable C5 to SAS backplane connector X9
  - SAS cable to backplane connectors X1

For a complete cabling overview, please refer to section "List of used cables" on page 331.

7.3.1.4 Concluding steps

- "Installing the fan box" on page 146
- "Reassembling" on page 57
- "Installing 2.5-inch HDD / SSD modules" on page 121
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- "Enabling BitLocker functionality" on page 88

7.3.2 Replacing the 12x 2.5-inch HDD SAS backplane

Field Replaceable Unit (FRU)

Hardware: 10 minutes

Tools:	Phillips PH2 / (+) No. 2 screw driver

7.3.2.1 Preliminary steps

The 2.5-inch HDD SAS backplane is mounted on the drive cages. It is not necessary to remove the drive cage before replacing the SAS / SATA backplane

- "Locating the defective server" on page 47
- "Disabling BitLocker functionality" on page 65
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50

- Remove all HDD / SSD modules from the server as described in section "Removing 2.5-inch HDD / SSD modules" on page 124.

  CAUTION!

  Ensure that all hard disk drives are uniquely identified so that you can reinsert them into their original bays after replacing the HDD backplane.

- "Getting access to the component" on page 51
- "Removing the fan box" on page 144

7.3.2.2 Removing the 12x2.5-inch HDD SAS backplane

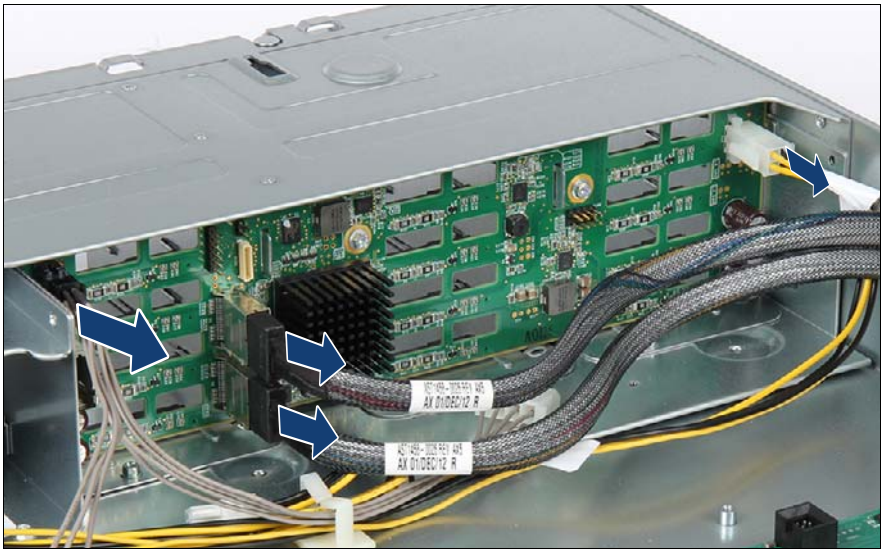


Figure 45: Disconnecting cables from the 12x 2.5-inch HDD SAS backplane

- Disconnect all cables from the 12x 2.5-inch HDD SAS backplane:
  - SAS cables
  - Power cables

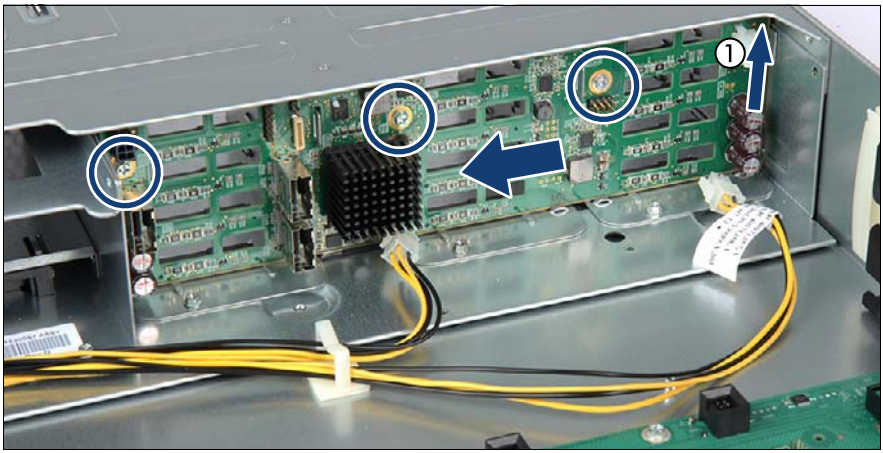


Figure 46: Removing the 2.5-inch HDD SAS backplane (A)

- ► Remove the three screws of the 12x 2.5-inch HDD SAS backplane (see circles).
- ► Shift the backplane slightly to the left to disengage the nose (1)

Figure 47: Removing the 2.5-inch HDD SAS backplane (B)

- ► Tilt out the 12x 2.5-inch HDD SAS backplane as shown.

► At a slight angle, unhinge the 12x 2.5-inch HDD SAS backplane from the guides on the drive cage and remove it.

7.3.2.3 Installing the 12x 2.5-inch HDD SAS backplane

Figure 48: Installing the 12x 2.5-inch HDD SAS backplane (A)

► At a slight angle, fit the 12x 2.5-inch HDD SAS backplane into the guides on the bottom of the chassis.

► Fold in the 12x 2.5-inch HDD SAS backplane.

► Shift it slightly to the right to engage the nose

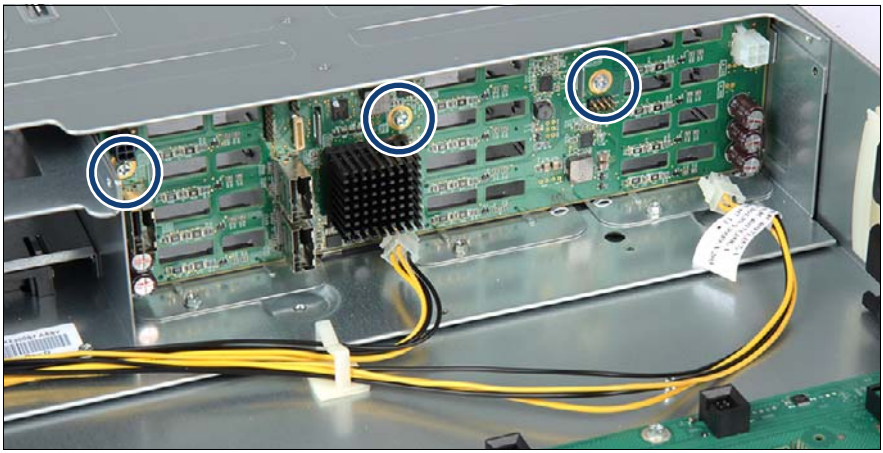


Figure 49: Fastening the 2.5-inch HDD SAS backplane (A)

► Secure the 12x 2.5-inch HDD SAS backplane with the three screws.

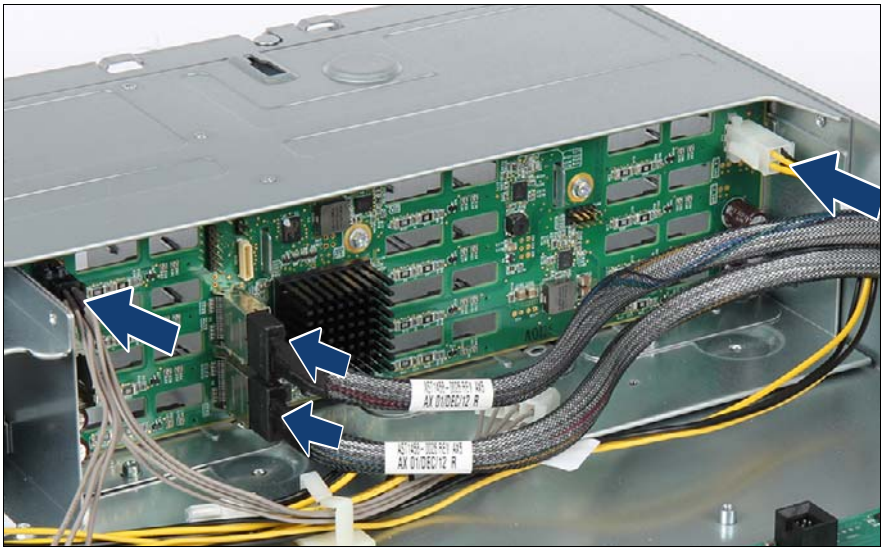


Figure 50: Connecting cables to the 12x 2.5-inch HDD SAS backplane

► Reconnect all cables to the 12x 2.5-inch HDD SAS backplane:

  – Power cable C4 connected to SAS backplane connector X15
  – Power cable C5 connected to SAS backplane connector X17

– SAS cable C9 connected to SAS controller connector MLC1 to primary backplane connectors X1

– SAS cable C9 connected to SAS controller connector MLC2 to secondary backplane connectors X2

For a complete cabling overview, please refer to section "List of used cables" on page 331.

7.3.2.4 Concluding steps

- "Installing the fan box" on page 146
- "Reassembling" on page 57
- "Installing 2.5-inch HDD / SSD modules" on page 121
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- "Enabling BitLocker functionality" on page 88

7.4 HDD cage

7.4.1 Removing a HDD cage

Field Replaceable Unit (FRU)

Hardware: 10 minutes

Tools:	Phillips PH2 / (+) No. 2 screw driver

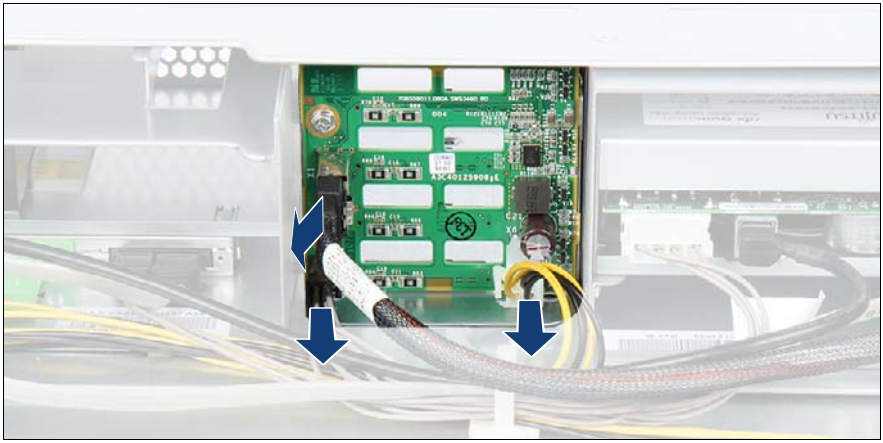


Figure 51: Disconnecting cables from the 4x 2.5-inch HDD SAS backplane

- ► Disconnect all cables from the 4x 2.5-inch HDD SAS backplane:
  - – SAS / SATA cable
  - – Power cables

Figure 52: Removing the 4x 2.5-inch HDD SAS backplane

- ► Remove the screw.
- ► Push the HDD cage out.

7.4.2 Installing a HDD cage

Field Replaceable Unit (FRU)

Hardware: 10 minutes

Tools:	Phillips PH2 / (+) No. 2 screw driver

Figure 53: Removing the 4x 2.5-inch HDD SAS backplane

- ► Insert the HDD cage.
- ► Fasten the HDD cage with the screw.

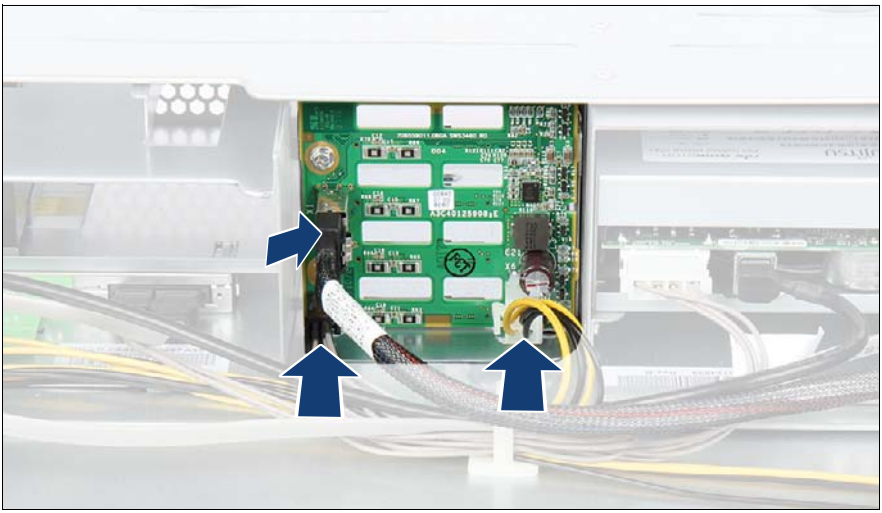


Figure 54: Reconnecting cables to the 4x 2.5-inch HDD SAS backplane

- ► Reconnect all cables to the 2.5-inch HDD SAS backplane:
  - – Power cable C4 to SAS backplane connector X6
  - – If applicable power cable C5 to SAS backplane connector X9
  - – SAS cable to backplane connectors X1

8 System fan

Safety notes

CAUTION!

- Do not damage or modify internal cables or devices. Doing so may cause a device failure, fire, or electric shock.
- Devices and components inside the server remain hot after shutdown. After shutting down the server, wait for hot components to cool down before installing or removing internal options.
- Circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. Always discharge static build-up (e.g. by touching a grounded object) before handling electrostatic-sensitive devices (ESDs).
- Do not touch the circuitry on boards or soldered parts. Hold circuit boards by their metallic areas or edges.
- If devices are installed or disassembled using methods other than those outlined in this chapter, the warranty will be invalidated.
- For further information, please refer to chapter "Important information" on page 35

8.1 Basic information

The following fans are available:

– five system fans included in a system fan box

– up to two fans, that are integral parts of the power supply units and cannot be replaced separately

The fan configuration is redundant. One fan may be faulty. Replace the fan as soon a possible. During the server is switched on, only one fan may be removed.

8.2 Replacing the system fan

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools:	tool-less

8.2.1 Preliminary steps

- "Locating the defective server" on page 47
- "Getting access to the component" on page 51
- "Locating the defective component" on page 49

8.2.2 Removing a system fan

Please notice the advices for redundancy!

Figure 55: Removing a system fan

- ► Take the system fan by the green touch points.
- ► Lift the system fan out of the fan box.

8.2.3 Installing a system fan

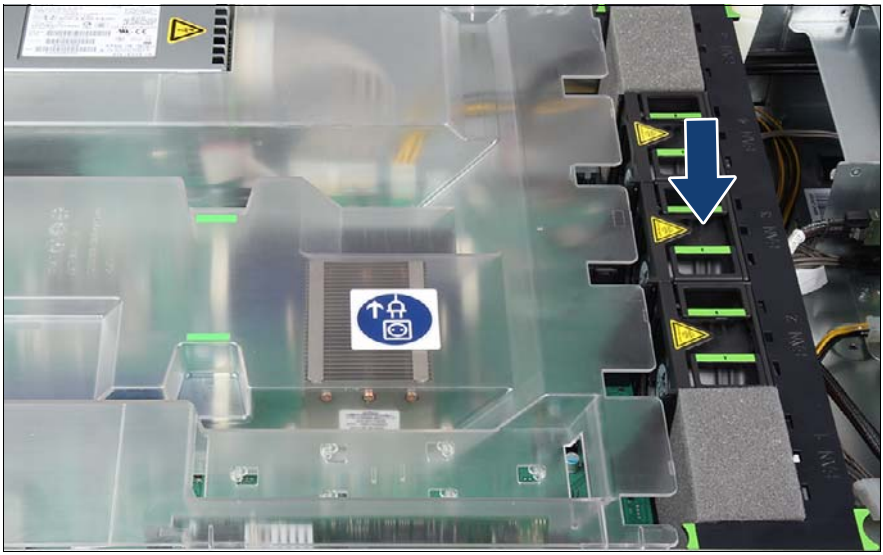


Figure 56: Installing a system fan module

- ► Insert the system fan as shown.
- ► Press down on the system fan until it locks.

8.2.4 Concluding steps

- ► "Reassembling" on page 57

i When a system fan module fails, the remaining fans will start operating at full speed. After the defective fan module has been replaced, all fans will continue to run at full speed for a couple of minutes, before resetting to a lower speed.

Ensure that all system fans reset to a normal operating speed.

- ► "Performing a fan test after replacing a defective fan" on page 93

8.3 Removing the fan box

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools: screw driver

8.3.1 Preliminary steps

- "Locating the defective server" on page 47
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

8.3.2 Removing the fan box

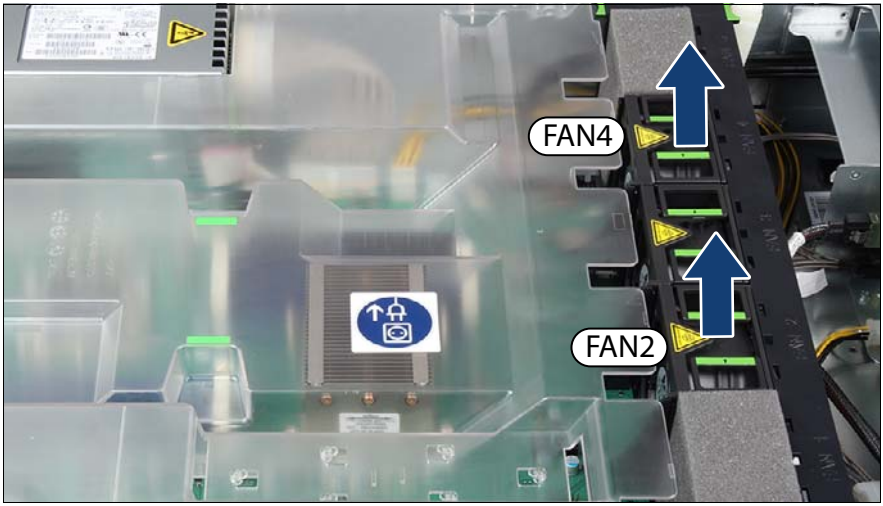


Figure 57: Removing a fan module

- Take the two system fans by the green touch points and lift the system fans out of the fan box.

Figure 58: Removing the fan box

► Remove the two screws.

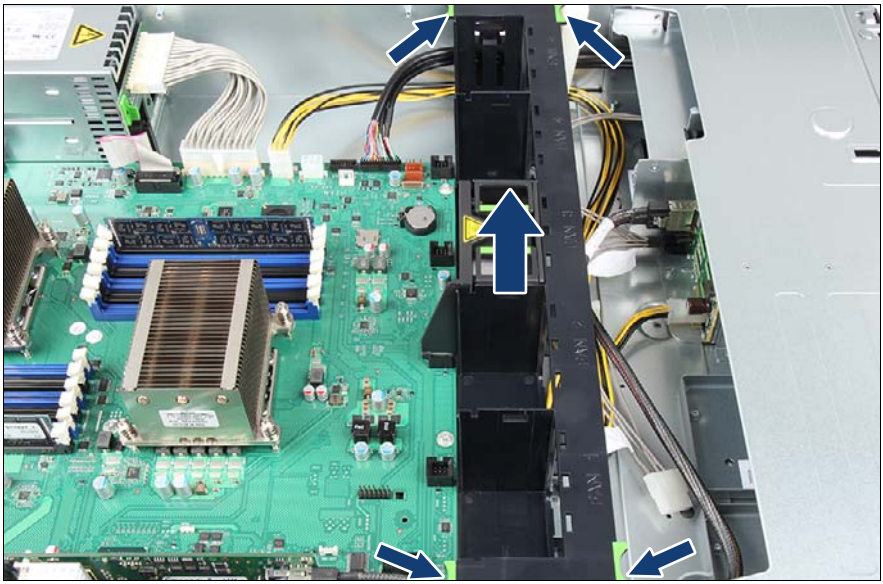


Figure 59: Removing the fan box

► Take the fan box by the green touch points and lift the fan box out of the chassis.

8.3.3 Installing the fan box

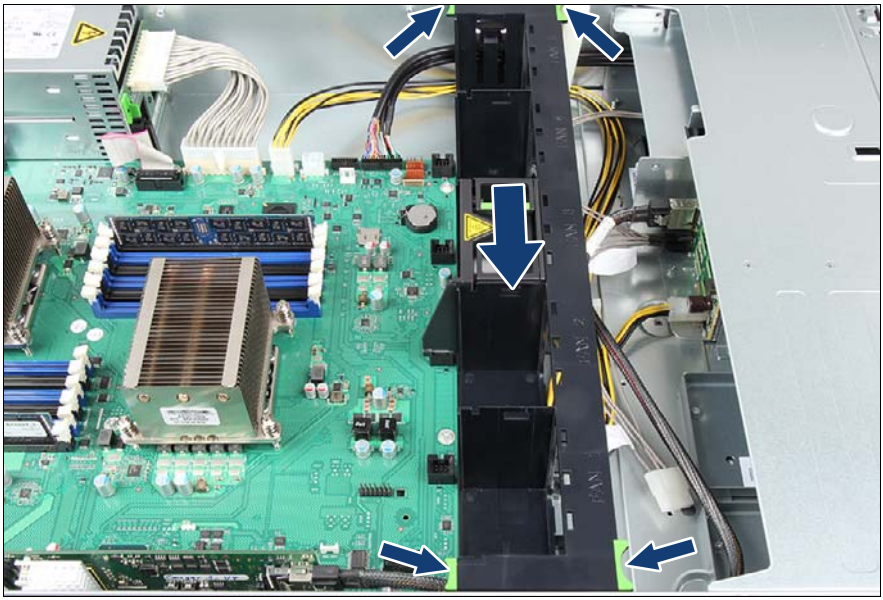


Figure 60: Installing the fan box

► Take the fan box by the green touch points and insert the fan box.

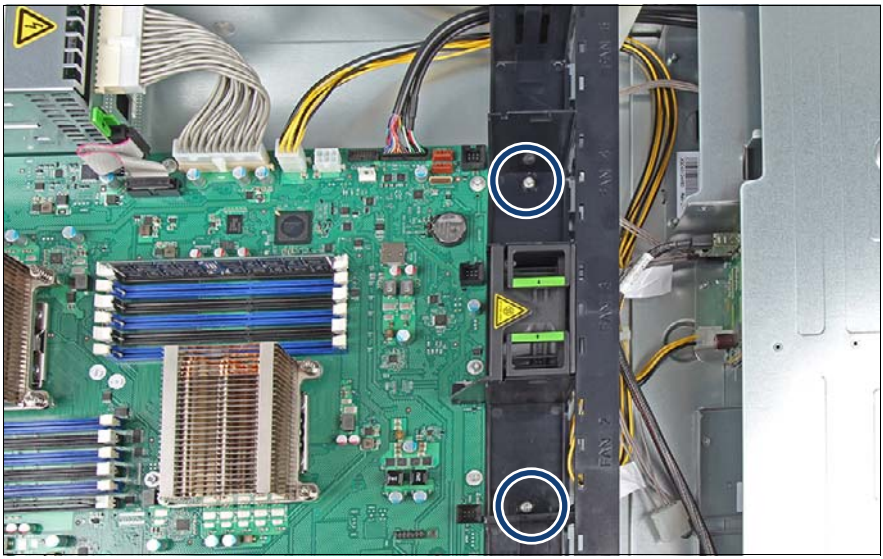


Figure 61: Installing the fan box

- Fasten the fan box with the 2 screws.
- Install the two fan modules see section "Installing a system fan" on page 143.

8.3.4 Concluding steps

- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64

9 Expansion cards and backup units

Safety notes

CAUTION!

- Do not damage or modify internal cables or devices. Doing so may cause a device failure, fire, or electric shock.
- Devices and components inside the server remain hot after shutdown. After shutting down the server, wait for hot components to cool down before installing or removing internal options.
- Circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. Always discharge static build-up (e.g. by touching a grounded object) before handling electrostatic-sensitive devices (ESDs).
- Do not touch the circuitry on boards or soldered parts. Hold circuit boards by their metallic areas or edges.
- If devices are installed or disassembled using methods other than those outlined in this chapter, the warranty will be invalidated.
- For further information, please refer to chapter "Important information" on page 35.

9.1 Basic information

The system board is equipped with seven expansion slots:

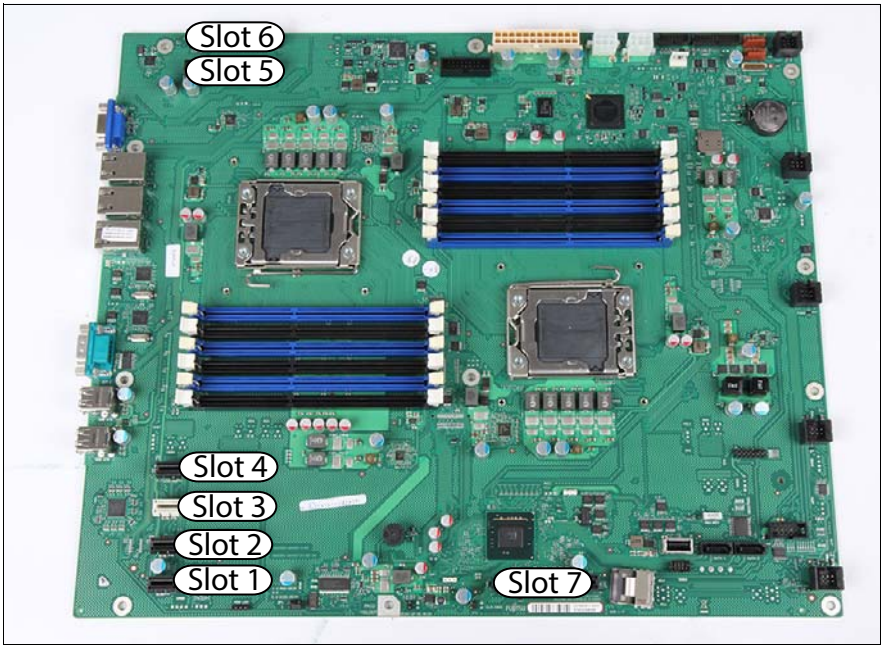


Figure 62: PCI slot overview

PCI slot	Type	Mechanical connector	Electrical interface	Function
1	PCIe Gen 2	x8	x4	preferred slot for Modular LAN controller (with NCSI connector) CPU1
2	PCIe Gen 3	x8	x8	CPU1
3	PCIe Gen 3	x8	x8	CPU1
4	PCIe Gen 3	x8	x8	only available with CPU2
5	PCIe Gen 3	x8	x8	only available with CPU2
6	PCIe Gen 3	x8	x8	only available with CPU2
7	PCIe Gen 3	x8	x8	slot for SAS RAID controller

Expansion card overview and installations sequence

Vendor/Type	Bus	Max#	Slot 1	Slot2	Slot3	Slot4	Slot5	Slot6	Slot7
VGA									
PCIe USB 3.0									
USB 3.0 PCIe x1 adapter card	x1 PCI1.0	1		1					
SAS/RAID									
RAID Ctrl SAS 6G 1GB (D3116C)	x8 PCI3.0	1							1
RAID Ctrl SAS 6G 5/6 512MB (D2616)	x8 PCI2.0	1							1
RAID Ctrl SAS 6G 0/1 (D2607)	X8 PCI2.0	1							1
RAID Ctrl SAS 6G 8Port ex 1 GB	x8 PCI3.0	2			1	2			
SAS(Backup)									
LSI SAS 9200-8e (3080)	x8 PCI2.0	3	6	4	5	1	2	3	
Fibre Channel									
LPe12002	x8 PCI1.0	4	6	4	5	1	2	3	
LPe1250	x8 PCI1.0	4	6	4	5	1	2	3	
QLE2560	x8 PCI1.0	4	6	4	5	1	2	3	
QLE2562	x8 PCI1.0	4	6	4	5	1	2	3	
Ethernet									
Eth Ctrl 2x10Gbit PCIe x8 D2755 SFP+	x8 PCI2.0	3	6	4	5	1	2	3	
Eth Ctrl 2x10GBase-T X540-T2	x8 PCI2.0	3	6	4	5	1	2	3	

Slot7: 1st Boot Slot Option ROM SCAN enabled = default
Slot3: 2nd Boot Slot Option ROM SCAN enabled = default
Slot4/5/6: CPU 2 must be installed to use slot4, 5 or 6

The list may be changed due to new controllers.

For the latest information on supported expansion cards, refer your server's hardware configurator available online at the following address:
for the EMEA market:
http://ts.fujitsu.com/products/standard_servers/index.htm
for the Japanese market:
http://jp.fujitsu.com/platform/server/primergy/system/

9.2 Handling slot brackets

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools:	Phillips PH2 / (+) No. 2 screw driver

9.2.1 Installing a slot bracket

9.2.1.1 Installing a standard slot bracket

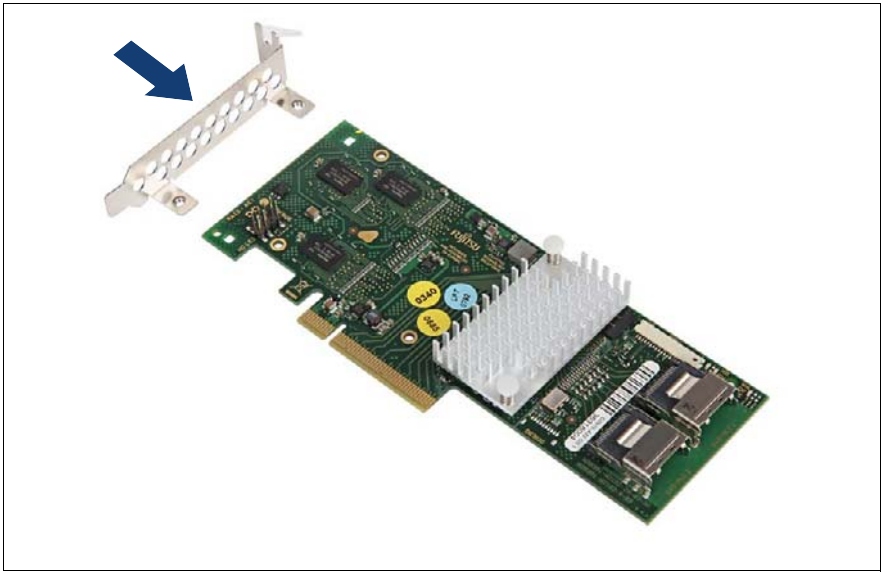


Figure 63: Installing a standard slot bracket (A)

► Place the controller on the mounting tabs on the slot bracket.

Figure 64: Installing a standard slot bracket (B)

► Secure the slot bracket to the controller with two M3 x 4.5 mm screws.

9.2.1.2 Installing a slot bracket to the Network adapter D2755

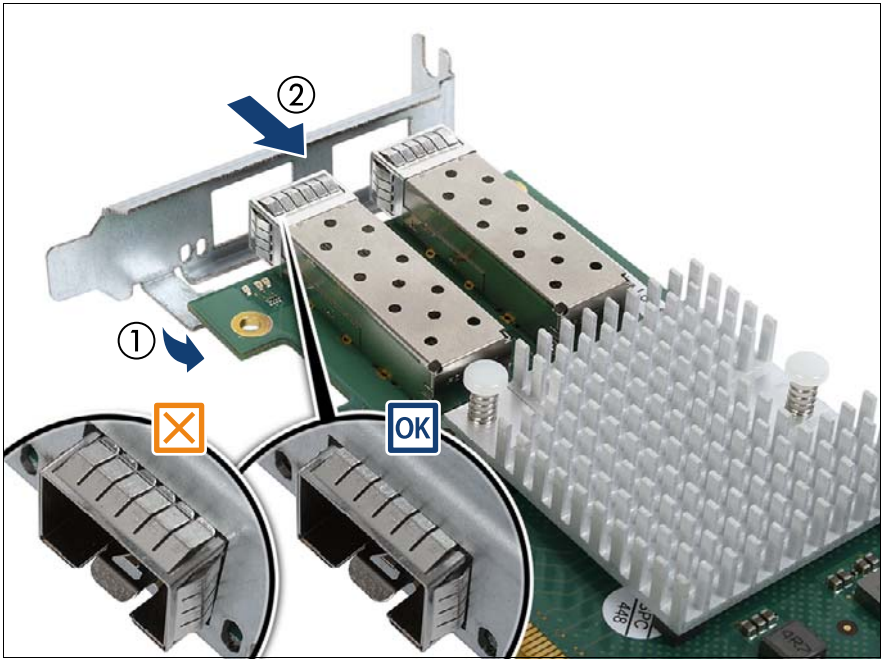


Figure 65: Network adapter D2755 - Mounting the slot bracket (A)

- ► Place the controller on the mounting tabs on the slot bracket (1).
- ► Carefully shift the slot bracket towards the controller until the plug shells engage with the cut-outs in the slot bracket connector panel (2).
- ► Ensure that the ESD springs on the plug shells properly engage with the slot bracket as shown (see close-ups).

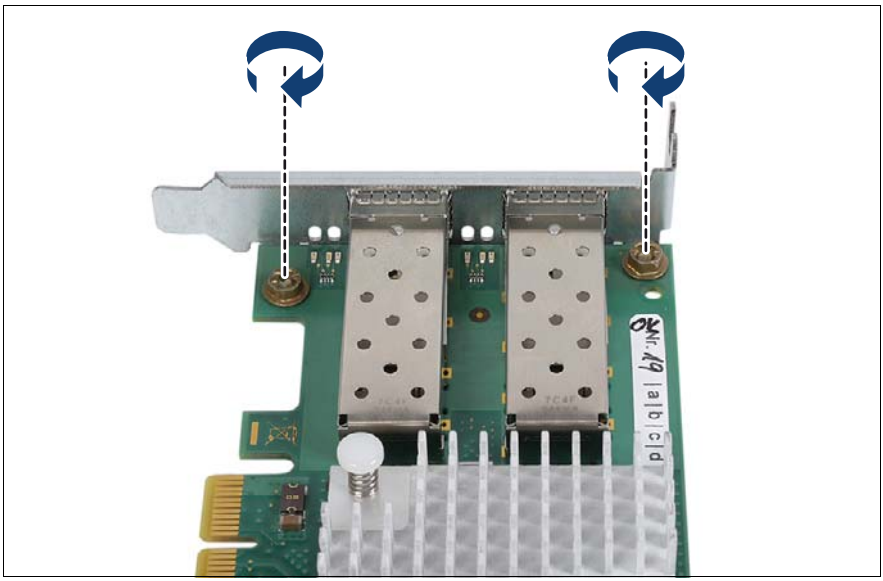


Figure 66: Network adapter D2755 - Mounting the slot bracket (B)

► Secure the slot bracket to the controller with two M3 x 4.5 mm screws.

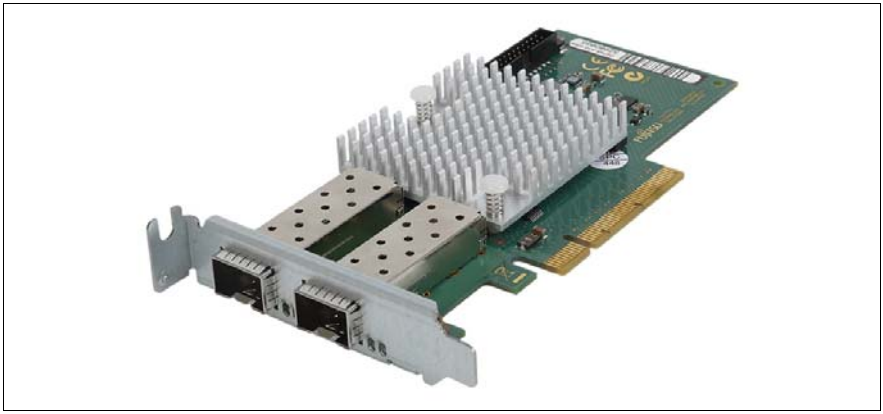


Figure 67: Network adapter D2755 - Mounting the slot bracket (C)

Assembled network adapter D2755

9.2.1.3 Installing a slot bracket to the USB 3.0 interface card D3305

CAUTION!

The USB 3.0 interface card D3305 comes pre-assembled with a full height slot bracket. When replacing the slot bracket, ensure to use the original M3 x 5 mm screws. Standard M3 screws may damage onboard components.

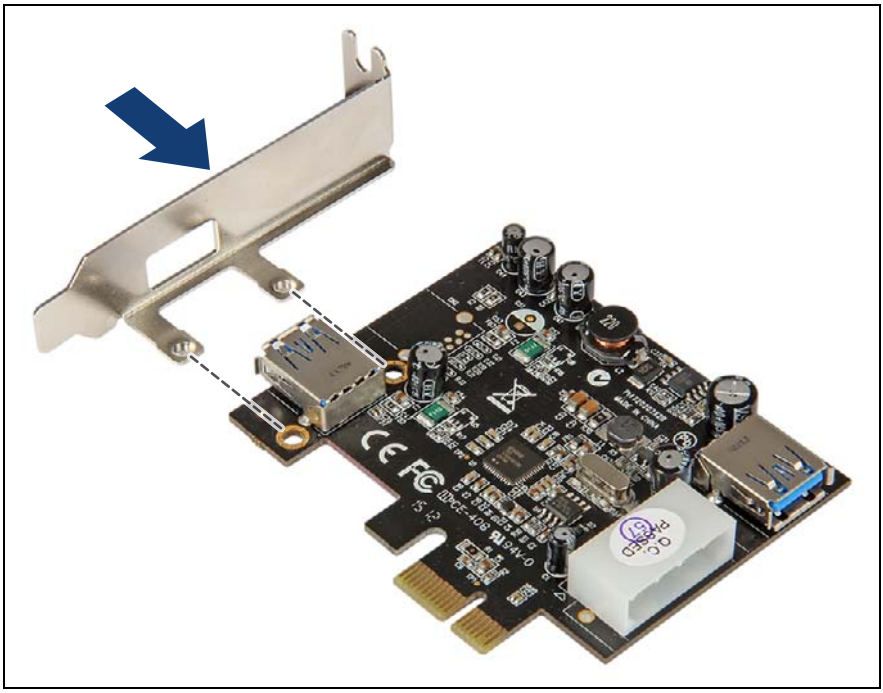


Figure 68: Mounting the slot bracket (A)

- ► Place the controller on the mounting tabs on the slot bracket.
- ► Carefully shift the slot bracket towards the controller until the plug shells engage with the cut-outs in the slot bracket connector panel.

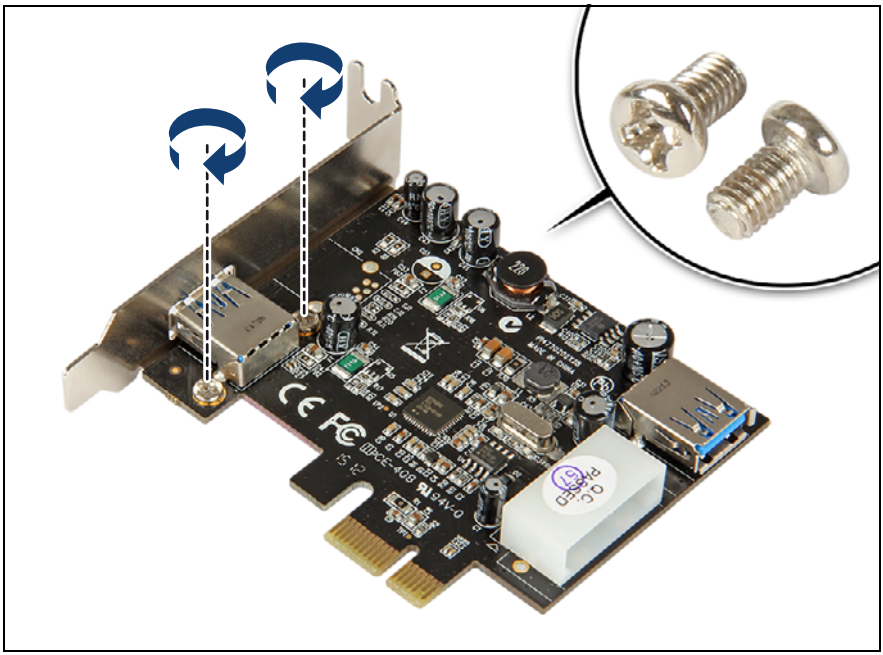


Figure 69: Mounting the PCI slot bracket (B)

- Secure the slot bracket to the controller with the two M3 x 5 mm screws contained in the expansion card kit.

9.2.2 Removing a slot bracket

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools:	Phillips PH2 / (+) No. 2 screw driver

Removing the slot bracket

- Remove the two screws.
- Remove the controller from the mounting tabs on the slot bracket.

9.3 Expansion cards

9.3.1 Installing expansion cards

Upgrade and Repair Unit (URU)

Hardware: 5 minutes
Software: 5 minutes

Tools:	Phillips PH2 / (+) No. 2 screw driver

9.3.1.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Disabling SVOM boot watchdog functionality" on page 66
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

9.3.1.2 Removing the slot bracket

Figure 70: Removing the slot bracket

- ► Remove the screw.
- ► Remove the slot bracket.

CAUTION!

Keep the slot bracket for further use.

Always replace slot brackets into unused PCI slot openings to comply with applicable EMC regulations and satisfy cooling requirements.

9.3.1.3 Installing an expansion card

- ► Remove the expansion card from its protective packaging.

For further instructions regarding controller settings, please refer to the accompanying documentation.

- ► If applicable, attach the required slot bracket to the expansion card as described in section "Installing a slot bracket" on page 153.

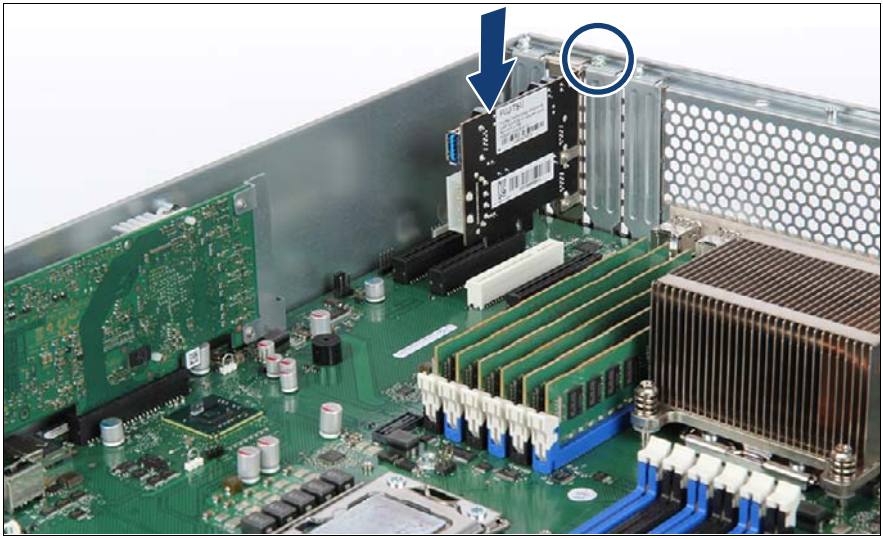


Figure 71: Installing the expansion card

- Carefully insert the expansion card into the desired PCI slot and press down firmly until it is fully seated in the slot.
- Fasten the expansion card with the screw.
- If applicable, install SFP+ transceiver modules into the new expansion card, as described in section "Installing SFP+ transceiver modules" on page 186.
- If applicable, connect internal cables to the expansion card.

  For a complete cabling overview, please refer to section "List of used cables" on page 331.
- If applicable, connect a FBU to the expansion card as described in section "Installing a FBU" on page 174.

9.3.1.4 Concluding steps

- "Reassembling" on page 57
- Reconnect all external cables to the expansion card.
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- "Updating RAID controller firmware" on page 77

- If applicable, "Enabling Option ROM scan" on page 78.
- "Enabling SVOM boot watchdog functionality" on page 82
- "Enabling BitLocker functionality" on page 88

9.3.2 Removing expansion cards

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools:	Phillips PH2 / (+) No. 2 screw driver

9.3.2.1 Preliminary steps

- "Locating the defective server" on page 47
- "Disabling BitLocker functionality" on page 65
- "Shutting down the server" on page 49
- Remove all external cables from the expansion card to be removed.
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

9.3.2.2 Removing an expansion card

- If applicable, disconnect internal cables from the expansion card.

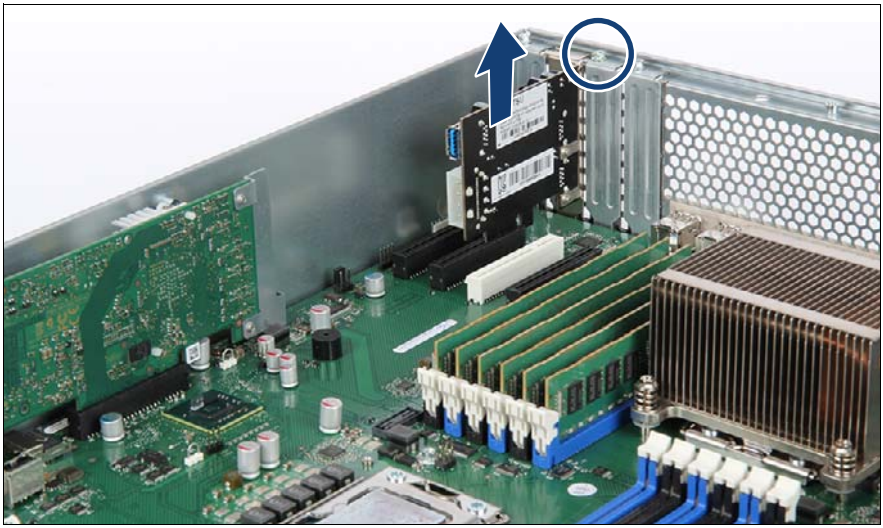


Figure 72: Removing an expansion card

- If applicable, "Removing an SFP+ transceiver module" on page 190.
- Remove the screw.
- Carefully remove the expansion card from its slot.

9.3.2.3 Installing a PCI slot bracket

CAUTION!

Always replace slot brackets into unused PCI slot openings to comply with applicable EMC regulations and satisfy cooling requirements.

Figure 73: Installing a slot bracket

- Insert a slot bracket into the unused PCI slot opening.
- Fasten slot bracket with the screw.

9.3.2.4 Concluding steps

- "Reassembling" on page 57
- "Mounting the housing cover" on page 59
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- "Enabling BitLocker functionality" on page 88

9.3.3 Replacing expansion cards

Upgrade and Repair Unit (URU)

Hardware: 5 minutes
Software: 5 minutes

Tools: Phillips PH2 / (+) No. 2 screw driver

Note on network settings recovery

When replacing network controllers or the system board, network configuration settings in the operating system will be lost and replaced by default values. This applies to all static IP address and LAN teaming configurations.

Ensure to note down your current network settings before replacing a controller or the system board.

9.3.3.1 Preliminary steps

- If applicable, "Note on network settings recovery" on page 165.
- "Disabling BitLocker functionality" on page 65
- "Disabling SVOM boot watchdog functionality" on page 66
- "Locating the defective server" on page 47
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- Remove all external cables from the expansion card to be replaced.
- "Getting access to the component" on page 51
- Locate the defective expansion card using the onboard Local Diagnostic LEDs as described in section "Onboard indicators and controls" on page 349.

9.3.3.2 Removing an expansion card

- If applicable, "Removing an SFP+ transceiver module" on page 190.
- "Removing expansion cards" on page 162

- If the slot bracket on the defective expansion card is to be reused, remove it from the board as described in section "Removing the slot bracket" on page 160.

9.3.3.3 Installing an expansion card

- If applicable, "Installing a slot bracket" on page 153.
- "Installing expansion cards" on page 159.
- If applicable, "Installing SFP+ transceiver modules" on page 186.

9.3.3.4 Connecting cables to the expansion card

- If applicable, connect internal cables to the expansion card.

  For a complete cabling overview, please refer to section "List of used cables" on page 331.

9.3.3.5 Connecting a battery backup unit to the expansion card

- If applicable, connect a FBU to the expansion card as described in section "Installing a FBU" on page 174.

9.3.3.6 Concluding steps

- "Reassembling" on page 57
- Reconnect all external cables to the replaced expansion card.
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- "Enabling replaced components in the system BIOS" on page 82
- Inform the customer about changed WWN and MAC addresses. For further information, refer to section "Looking up changed MAC / WWN addresses" on page 89.
- "Updating RAID controller firmware" on page 77
- "Enabling SVOM boot watchdog functionality" on page 82
- "Enabling BitLocker functionality" on page 88

9.4 SAS RAID controller in PCI slot 7

9.4.1 Installing the SAS RAID controller

Upgrade and Repair Unit (URU)

Hardware: 10 minutes
Software: 5 minutes

Tools:	Phillips PH2 / (+) No. 2 screw driver

9.4.1.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Disabling SVOM boot watchdog functionality" on page 66
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

9.4.1.2 Preparing the SAS RAID controller

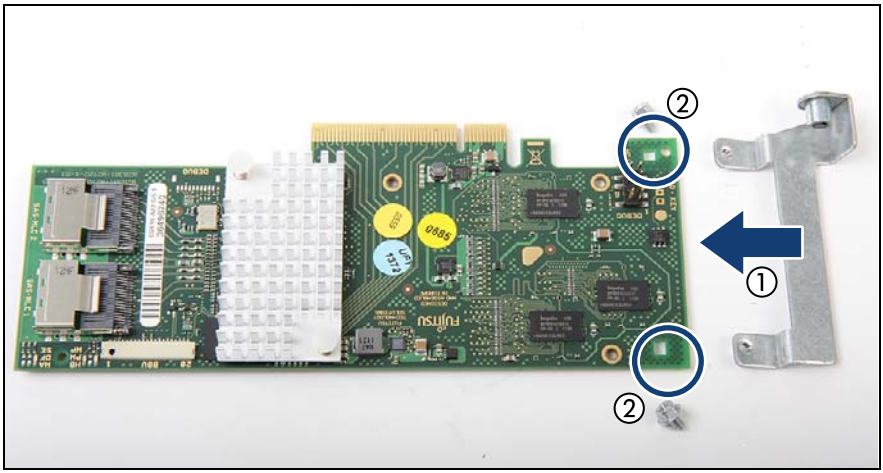


Figure 74: Installing the RAID card holder

- ► Place the controller on the mounting tabs on the slot bracket (1).
- ► Secure the slot bracket to the controller with two M3 x 4.5 mm screws (2).

9.4.1.3 Installing the SAS RAID controller

- ► Remove the SAS RAID controller from its protective packaging.

  For further instructions regarding controller settings, please refer to the accompanying documentation.

- ► If applicable, attach the required slot bracket to the expansion card as described in section "Preparing the SAS RAID controller" on page 167.

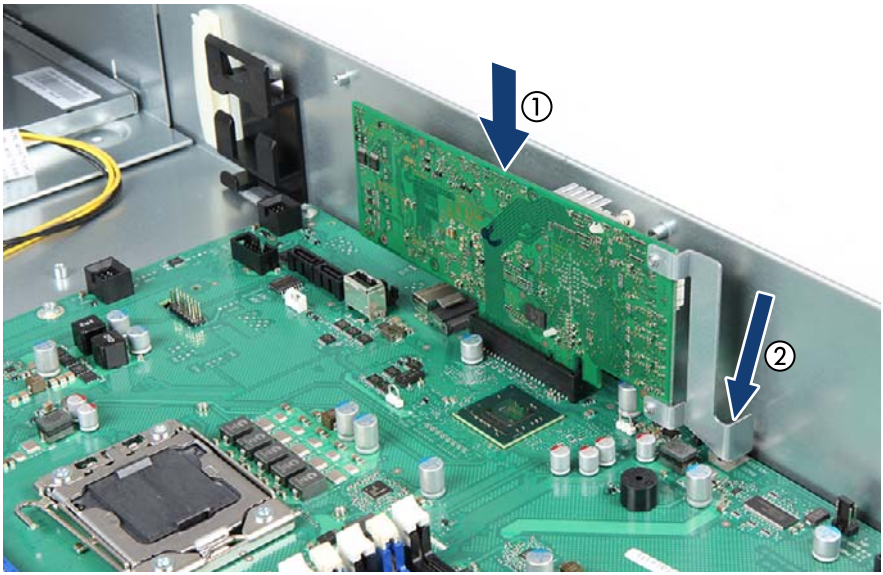


Figure 75: Installing the SAS RAID controller

- ► Carefully insert the RAID controller into PCI slot 7 and press down firmly until it is fully seated in the slot (1).

  For slot preferences, please refer to section "Basic information" on page 149.

- ► Secure the RAID controller with the screw on the RAID card holder (2).

9.4.1.4 Connecting cables to the expansion card

► Connect SAS cables to the SAS RAID controller.

For a complete cabling overview, please refer to section "List of used cables" on page 331.

9.4.1.5 Connecting a backup unit to the expansion card

► If applicable, connect a FBU to the expansion card as described in section "Installing a FBU" on page 174.

9.4.1.6 Concluding steps

► "Reassembling" on page 57

► "Connecting the server to the power source" on page 62

► "Switching on the server" on page 64

► In order to configure an expansion card that has been installed or replaced, the card's Option ROM has to be enabled in the system board BIOS. If applicable, proceed as described in section "Enabling Option ROM scan" on page 78.

► "Enabling SVOM boot watchdog functionality" on page 82

► "Enabling BitLocker functionality" on page 88

► "Updating RAID controller firmware" on page 77

9.4.2 Removing the SAS RAID controller

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools:	Phillips PH2 / (+) No. 2 screw driver

9.4.2.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Disabling SVOM boot watchdog functionality" on page 66
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

9.4.2.2 Removing the SAS RAID controller

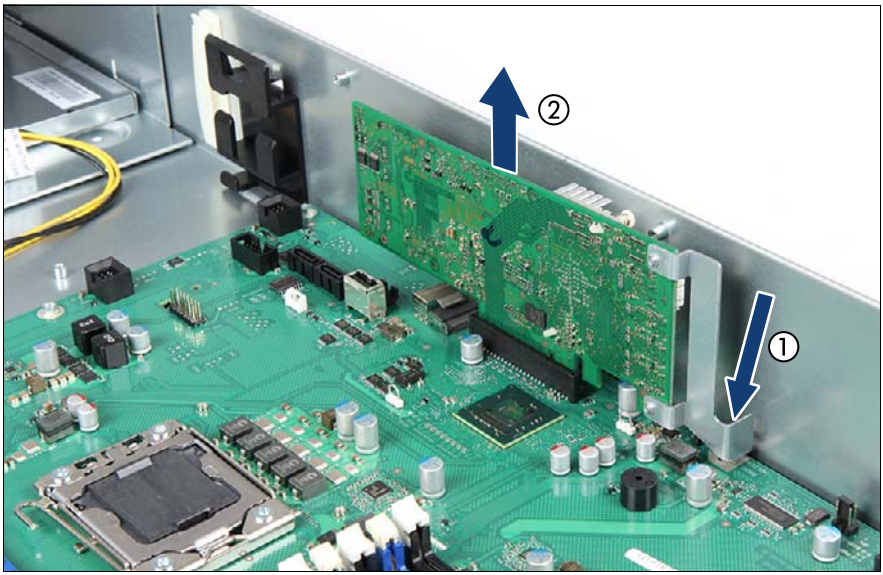


Figure 76: Removing the SAS RAID controller

- Loosen the screw on the RAID card holder (1).
- Carefully pull up on the SAS RAID controller in a vertical motion and remove it from its slot (2).

9.4.2.3 Removing the SAS RAID card holder

Figure 77: **Removing the RAID card holder**

- Remove the screws(1).
- Remove the slot bracket (2).

9.4.2.4 Concluding steps

- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- In order to configure an expansion card that has been installed or replaced, the card's Option ROM has to be enabled in the system board BIOS. If applicable, proceed as described in section "Enabling Option ROM scan" on page 78.
- "Enabling SVOM boot watchdog functionality" on page 82
- "Enabling BitLocker functionality" on page 88
- "Updating RAID controller firmware" on page 77

9.4.3 Replacing the SAS RAID controller

Upgrade and Repair Unit (URU)

Hardware: 5 minutes
Software: 5 minutes

Tools: Phillips PH2 / (+) No. 2 screw driver

9.4.3.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Disabling SVOM boot watchdog functionality" on page 66
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

9.4.3.2 Removing the defective SAS RAID controller

- "Removing the SAS RAID controller" on page 170
- If the RAID card holder on the defective controller is to be reused, remove it from the board as described in section "Removing the SAS RAID card holder" on page 171.

9.4.3.3 Installing the new SAS RAID controller

- If applicable, install the RAID card holder on the new SAS RAID controller as described in section "Preparing the SAS RAID controller" on page 167.
- "Installing the SAS RAID controller" on page 167

9.4.3.4 Connecting cables to the expansion card

- Connect SAS cables to the SAS RAID controller.

  For a complete cabling overview, please refer to section "List of used cables" on page 331.

9.4.3.5 Connecting a backup unit to the expansion card

- If applicable, connect a FBU to the expansion card as described in section "Installing a FBU" on page 174.

9.4.3.6 Concluding steps

- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- In order to configure an expansion card that has been installed or replaced, the card's Option ROM has to be enabled in the system board BIOS. If applicable, proceed as described in section "Enabling Option ROM scan" on page 78.
- "Enabling SVOM boot watchdog functionality" on page 82
- "Enabling BitLocker functionality" on page 88
- "Updating RAID controller firmware" on page 77

9.5 Backup Units

9.5.1 Basic information

The Flash Backup Unit (FBU) backs up the memory contents of the connected SAS RAID controller in the event of a power failure. The PRIMERGY RX2520 M1 server can accommodate up to two backup units.

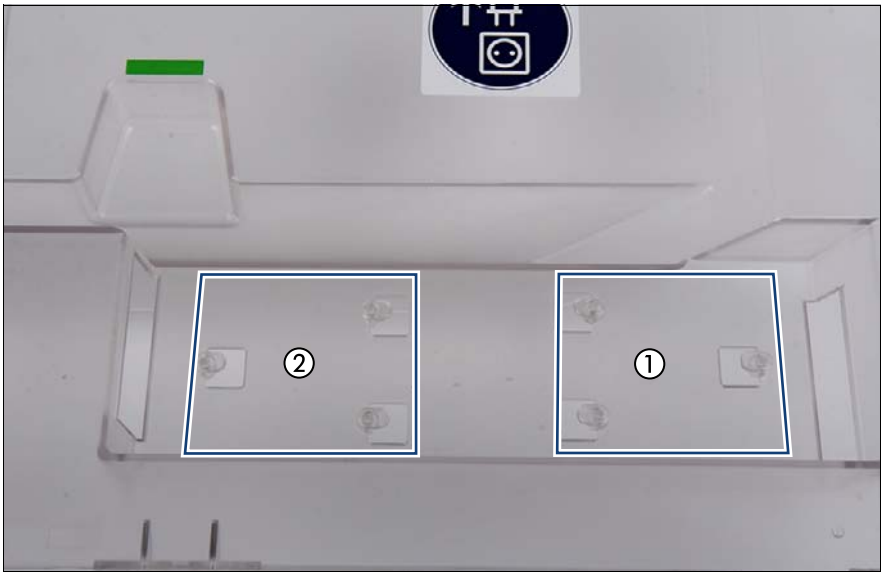


Figure 78: FBU mounting positions

1	Mounting position for first FBU
2	Mounting position for second FBU

9.5.2 Installing a FBU

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools:	Phillips PH1 / (+) No. 1 screw driver

CAUTION!

For further safety information, please refer to chapter "Important information" on page 35.

9.5.2.1 Preliminary steps

- "Disabling SVOM boot watchdog functionality" on page 66
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

9.5.2.2 Installing TFM to the RAID controller (if applicable)

To connect an FBU to the controller D3116 you need a TFM. Other controllers so as D9286CV-8e can be connected directly.

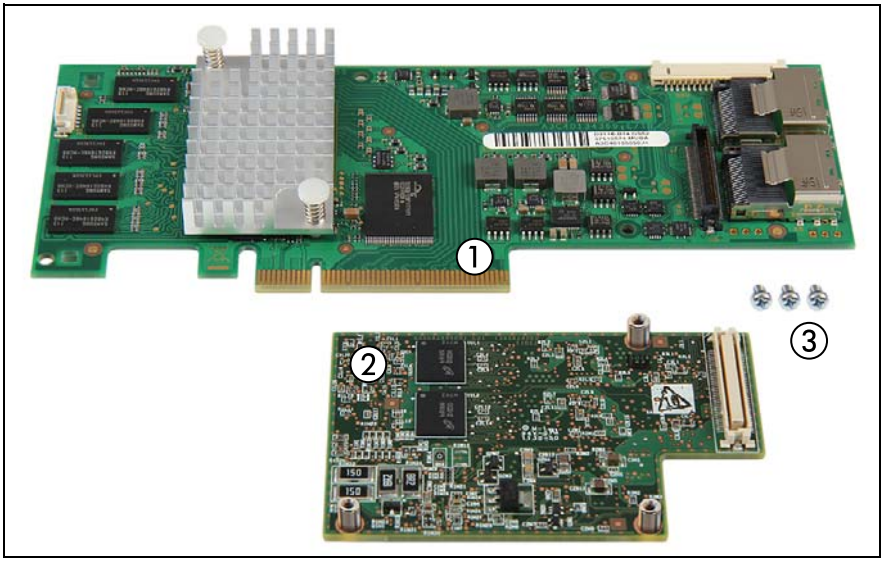


Figure 79: SAS RAID controller and TFM kit

1 SAS RAID controller D3116

2-3 TFM kit including three pre-assembled spacer bolts and three screws

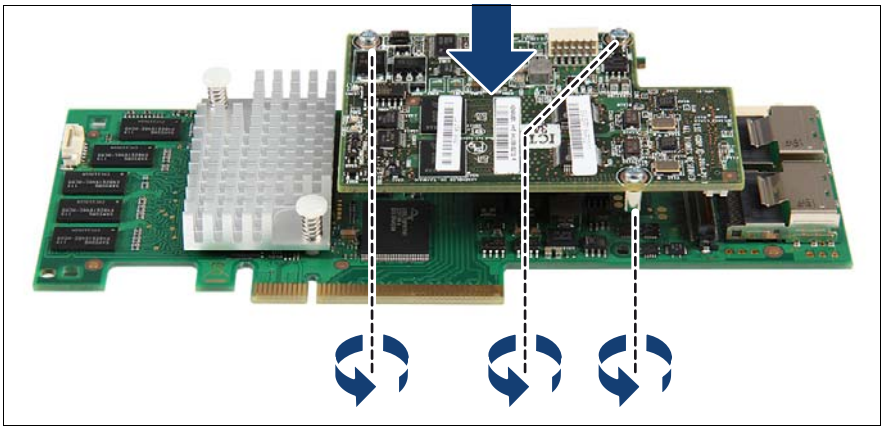


Figure 80: Mounting the TFM kit (A)

- ► Fit the spacer bolts on the TFM on SAS RAID controller.
- ► Secure the TFM on the controller with the three screws .

9.5.2.3 Preparing the FBU

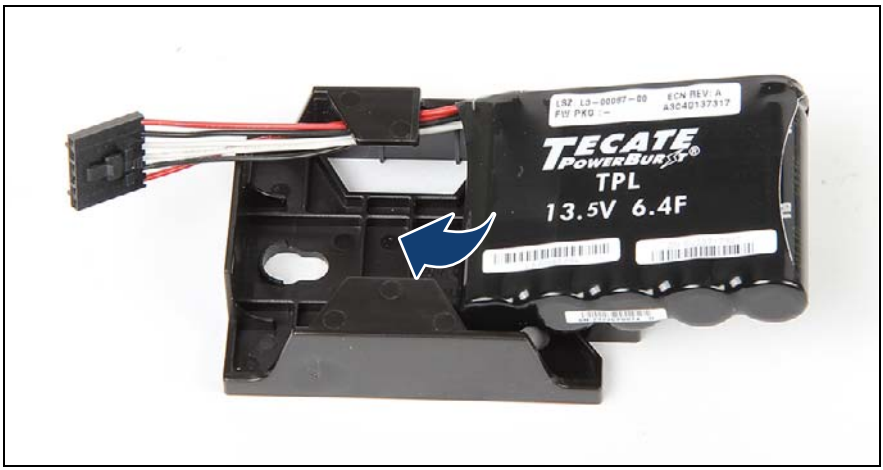


Figure 81: Installing the FBU in the FBU holder (A)

- ► At a slight angle, fit the FBU under both retaining brackets of the FBU holder as shown.
- ► Push in the FBU until it locks in place.

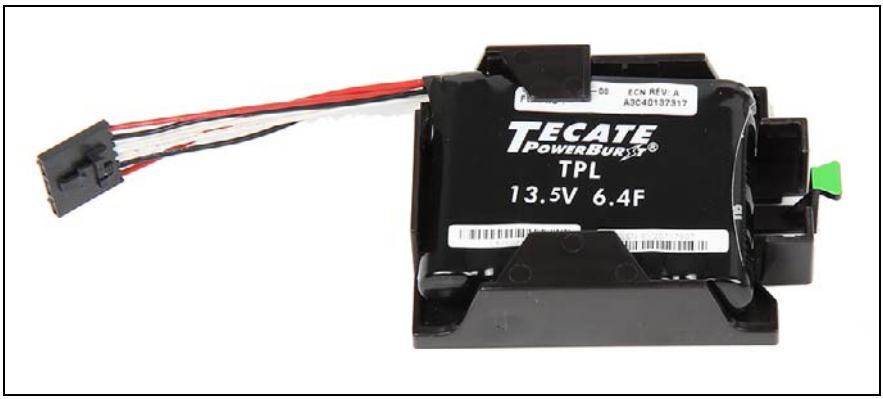


Figure 82: Installing the FBU in the FBU holder (B)

► Ensure that the FBU is properly seated in the holder.

9.5.2.4 Connecting the FBU cable to the FBU

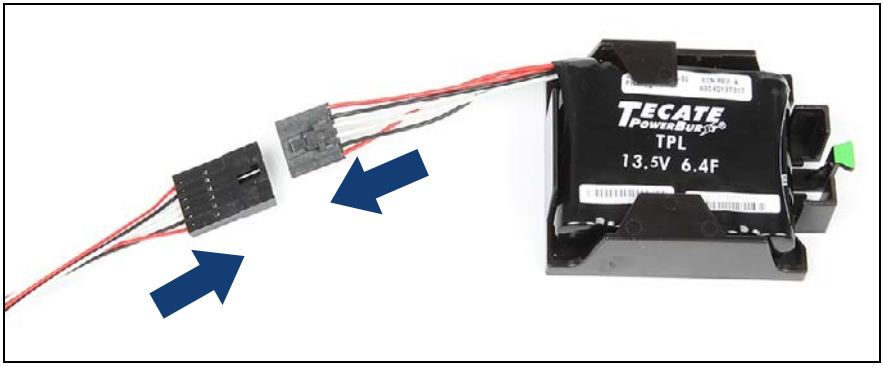


Figure 83: Connecting the FBU adapter cable to the FBU

► Connect the cable end on the FBU module to the FBU adapter cable as shown.

9.5.2.5 Installing the FBU holder onto the air duct

Figure 84: Installing the FBU holder (A)

Note the positions of the fixation bolts on the air duct and keyhole slots on the FBU holder.

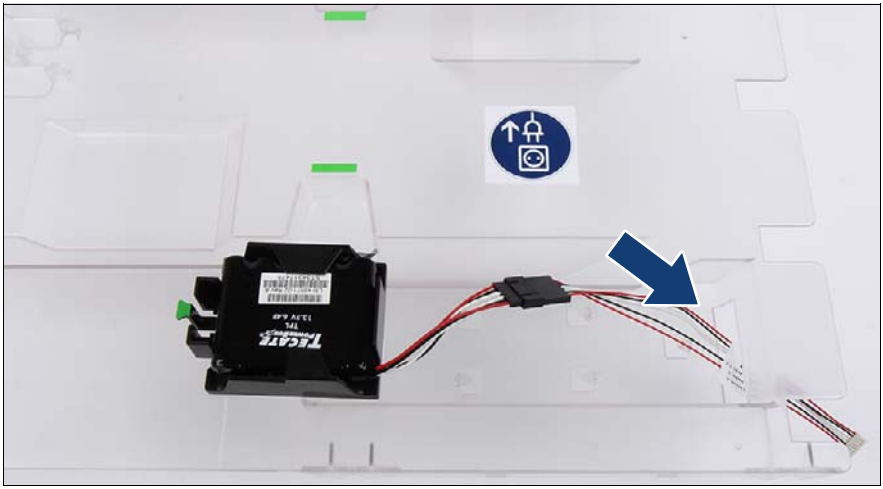


Figure 85: Installing the FBU holder (B)

► Thread the FBU cable through the gap in the air duct.

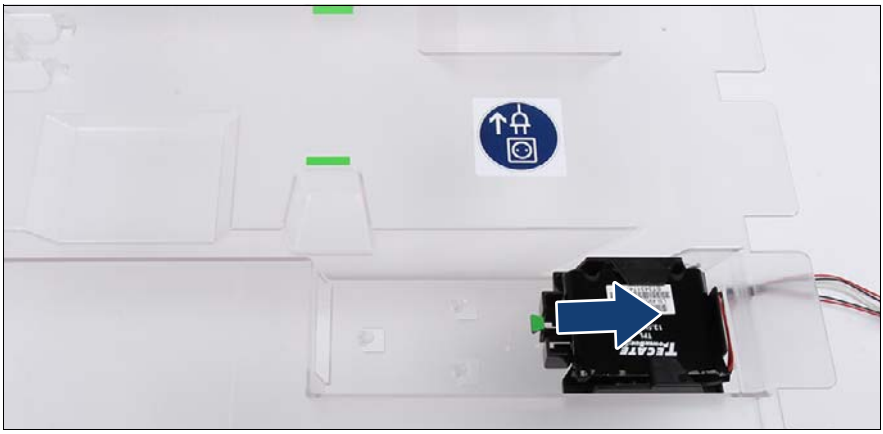


Figure 86: Installing the FBU holder (C)

- ► Insert the FBU holder into the air duct so that the three hooks on the air duct rest in the wide ends of the keyhole slots on the FBU holder.
- ► Slide the FBU holder in as far as it will go.

  The hooks on the air duct will lock in the narrow ends of the keyhole slots on the FBU holder.
- ► Ensure that the locking handle on the FBU holder properly snaps in place (3).

9.5.2.6 Installing the air duct with an FBU

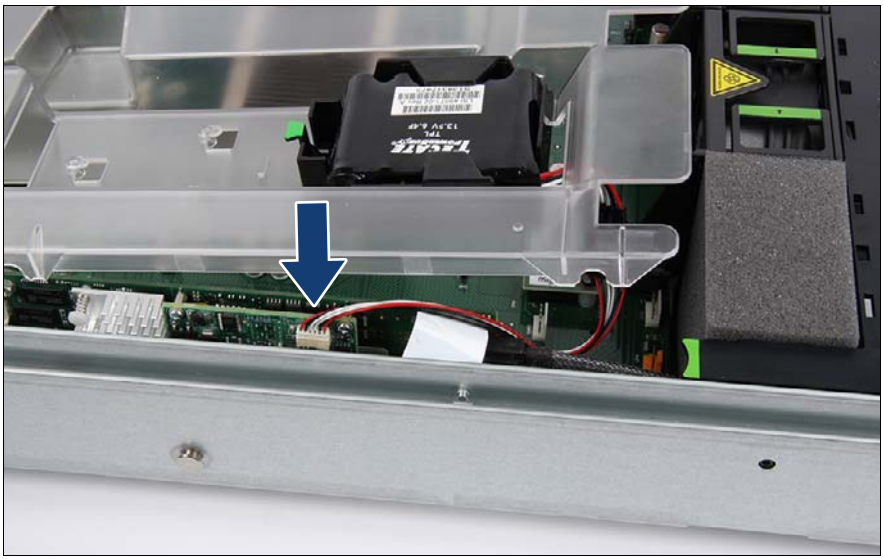


Figure 87: Connecting the FBU to the controller

- Insert the air duct.
- Connect the FBU cable to the RAID controller.
- Route the cable in such a way that the cable is not pinched under the air duct.

9.5.2.7 Concluding steps

- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- If applicable, "Updating RAID controller firmware" on page 77.
- "Enabling SVOM boot watchdog functionality" on page 82

9.5.3 Removing a FBU

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools: tool-less

CAUTION!

Do not throw backup units into the trash can. Batteries must be disposed of in accordance with local regulations concerning special waste.

For further safety information, please refer to section "Environmental protection" on page 45.

9.5.3.1 Preliminary steps

- "Disabling SVOM boot watchdog functionality" on page 66
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

9.5.3.2 Removing the air duct with an FBU

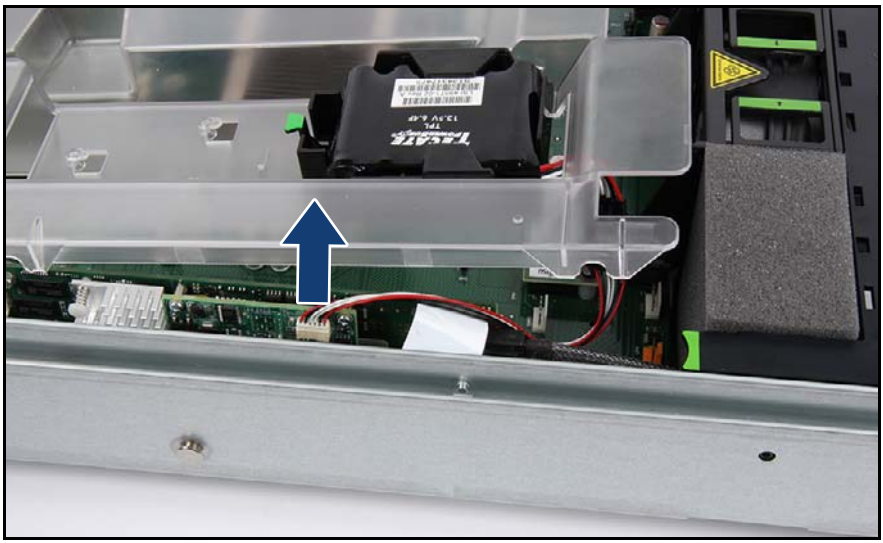


Figure 88: Disconnecting the FBU cable

► Carefully disconnect the FBU cable from the RAID controller (see arrow).

9.5.3.3 Removing the FBU holder from the air duct

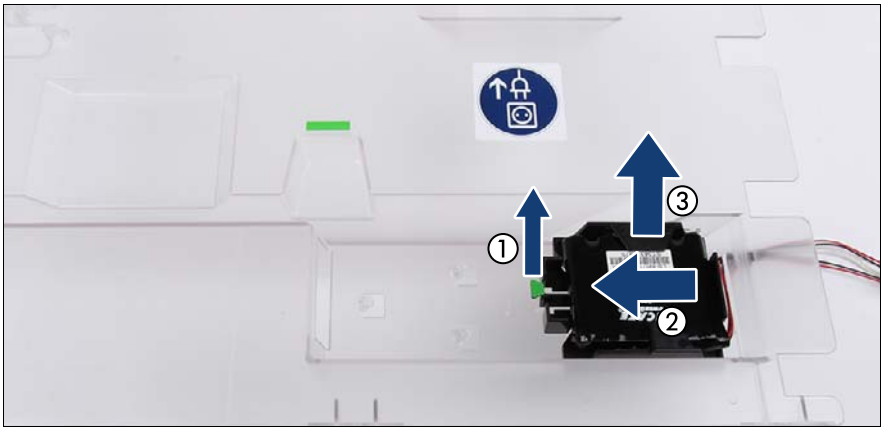


Figure 89: Removing the FBU holder from the air duct

- ► Lift up the green locking handle on the FBU holder (1) while sliding the FBU holder to the left as far as it will go (2).

  After that, the hooks on the air duct will rest in the wide ends of the keyhole slots on the holder.

- ► Lift the FBU holder from the air duct (3).
- ► Pull the FBU cable through the gap in the air duct.

9.5.3.4 Concluding steps

- ► "Reassembling" on page 57
- ► "Connecting the server to the power source" on page 62
- ► "Switching on the server" on page 64
- ► If applicable, "Updating RAID controller firmware" on page 77.
- ► "Enabling SVOM boot watchdog functionality" on page 82

9.5.4 Replacing a FBU

Upgrade and Repair Unit (URU)

Hardware: 10 minutes

Tools: tool-less

CAUTION!

Do not throw battery backup units into the trash can. Batteries must be disposed of in accordance with local regulations concerning special waste.

For further safety information, please refer to section "Environmental protection" on page 45.

9.5.4.1 Preliminary steps

- ► "Locating the defective server" on page 47
- ► "Disabling SVOM boot watchdog functionality" on page 66

- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

9.5.4.2 Removing a FBU from the air duct

- "Removing the FBU holder from the air duct" on page 182

9.5.4.3 Disconnecting the FBU cable from the FBU

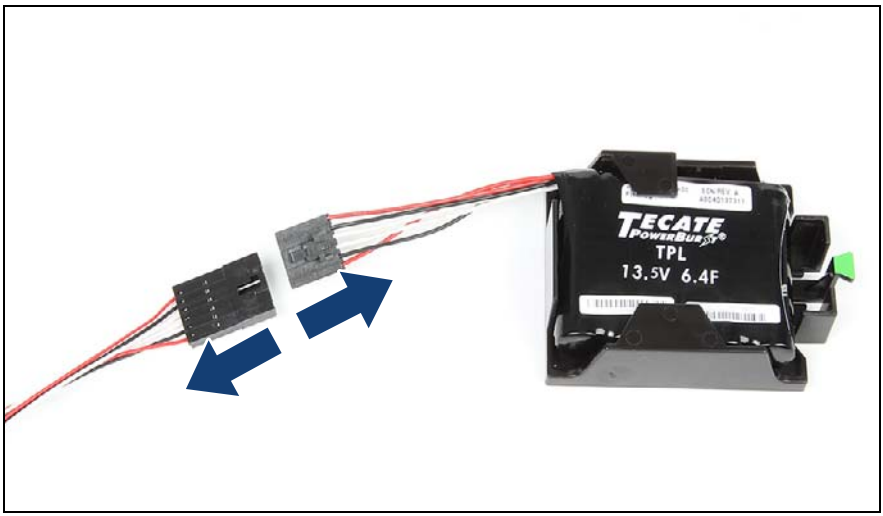


Figure 90: Disconnecting the FBU adapter cable from the FBU

- Press down on the locking latch on the FBU cable and disconnect the FBU adapter cable.

9.5.4.4 Removing the FBU from the holder

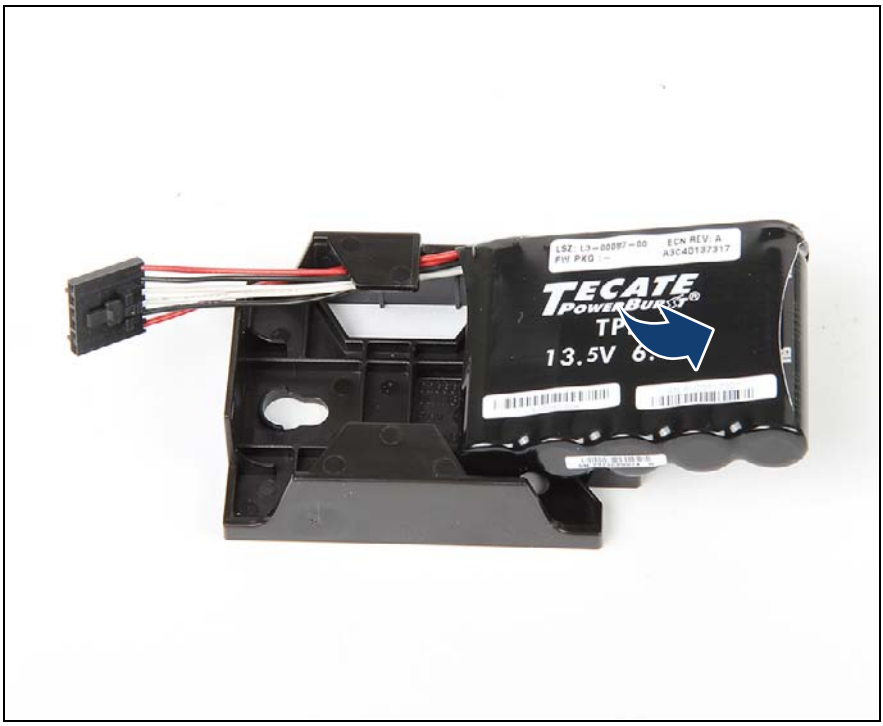


Figure 91: Removing the FBU from the holder

► Pull the FBU at a slight angle out of the holder.

9.5.4.5 Installing a new FBU

► "Connecting the FBU cable to the FBU" on page 177
► "Preparing the FBU" on page 176
► "Installing the FBU holder onto the air duct" on page 178

9.5.4.6 Concluding steps

► "Reassembling" on page 57
► "Connecting the server to the power source" on page 62

- "Switching on the server" on page 64
- If applicable, "Updating RAID controller firmware" on page 77.
- "Enabling SVOM boot watchdog functionality" on page 82

9.6 Handling SFP+ transceiver modules

For Fiber Channel over Ethernet (FCoE) configurations, the Ethernet server adapter is equipped with one or two SFP+ (small form-factor pluggable) transceiver modules.

9.6.1 Installing SFP+ transceiver modules

Upgrade and Repair Unit (URU) **Hardware: 5 minutes**

Tool:	tool-less

Preparing the SFP+ transceiver module

Figure 92: Removing the protective optical port plug

- ► Remove the SFP+ transceiver module from its protective packaging.
- ► Remove the optical port plug from the new / additional SFP+ transceiver module.

CAUTION!

– Always keep the protective port plugs attached to the transceiver optical bores and fiber-optic cable connectors until you are ready to make a connection.

– Save the protective port plug for future use.

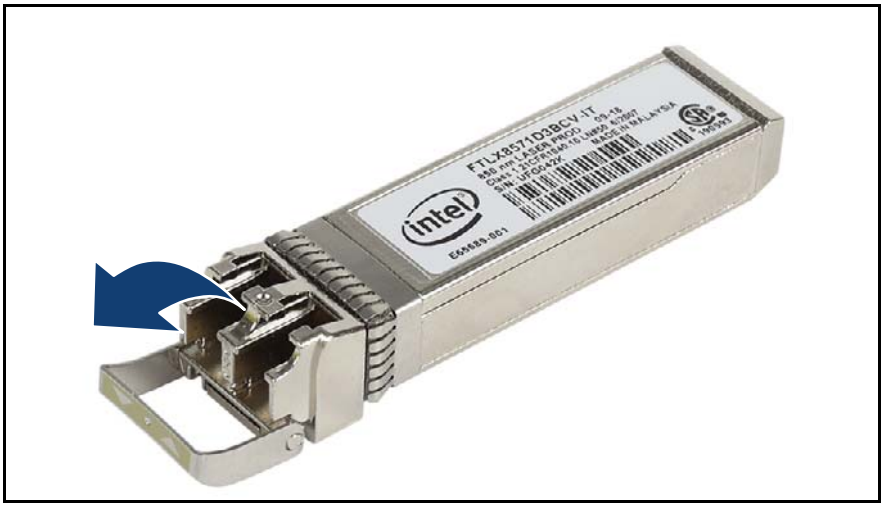


Figure 93: Unlatching the locking bail

- ► Carefully unlatch and fold down the locking bail on the SFP+ transceiver module.

Inserting the SFP+ transceiver module

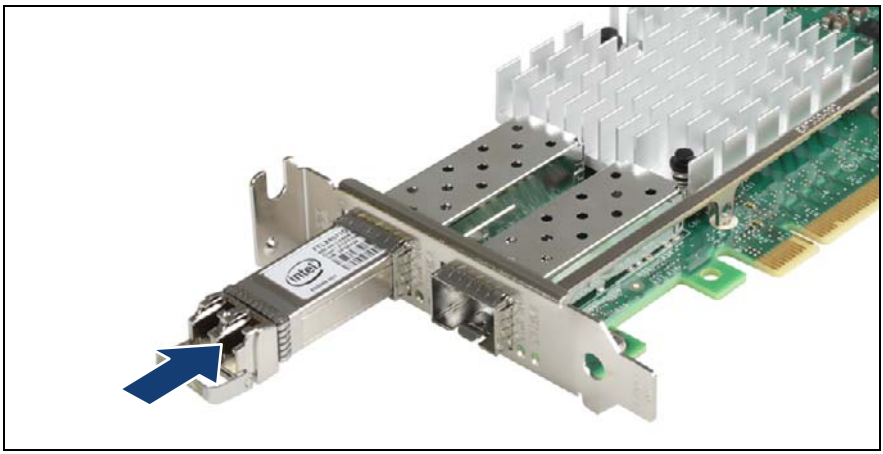


Figure 94: Inserting the SFP+ transceiver module

- Insert and slide the SFP+ transceiver module into the socket connector as far as it will go.

  If only one slot is equipped with a SFP+ transceiver module, use the primary connector as shown.

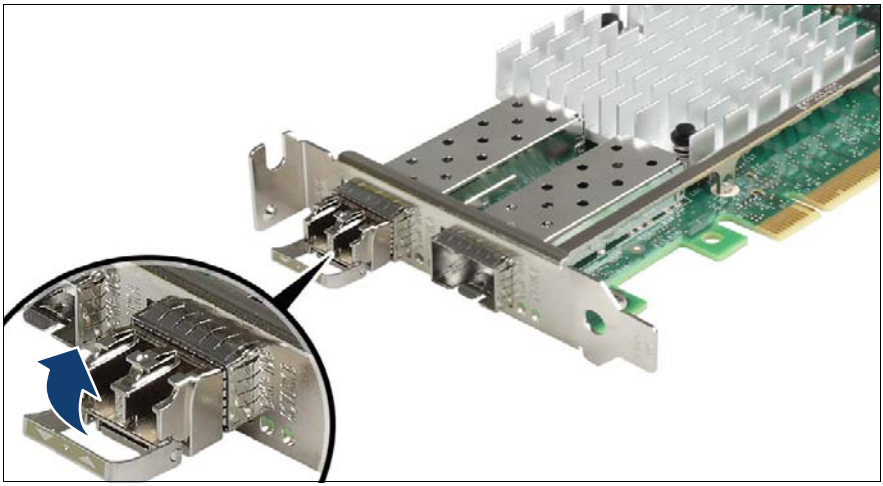


Figure 95: Latching the locking bail

► Carefully fold up and latch the locking bail.

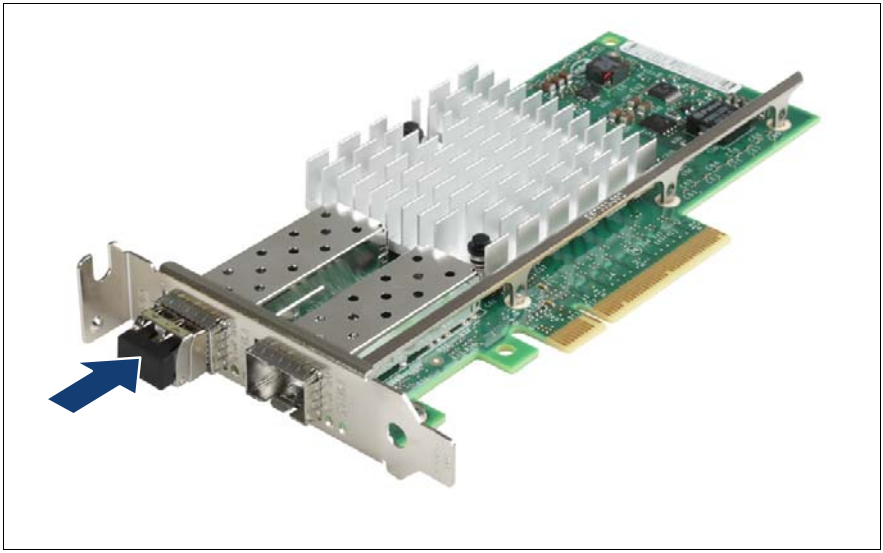


Figure 96: Attaching the protective optical port plug

► If the SFP+ transceiver module is not immediately connected to an LC connector, attach the protective optical port plug to the transceiver optical bores.

Installing the secondary SFP+ transceiver module

Figure 97: Installing the secondary SFP+ transceiver module

► If applicable, install the secondary SFP+ transceiver module accordingly.

9.6.2 Removing an SFP+ transceiver module

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tool:	tool-less

For Fiber Channel over Ethernet (FCoE) configurations, the ethernet server adapter is equipped with one or two SFP+ (small form-factor pluggable) transceiver modules.

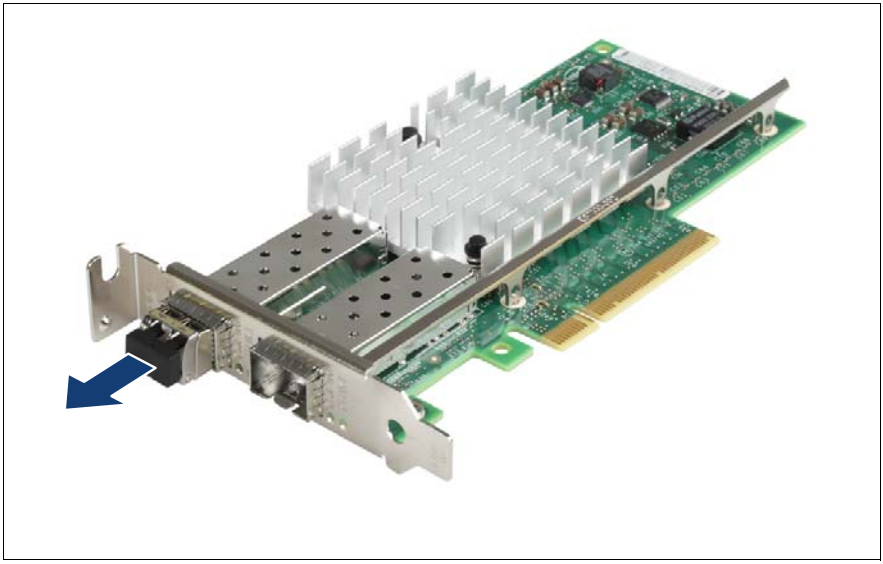


Figure 98: Removing the protective optical port plug

► If present, remove the protective optical port plug from the SFP+ transceiver module.

CAUTION!

Save the protective port plug for future use.

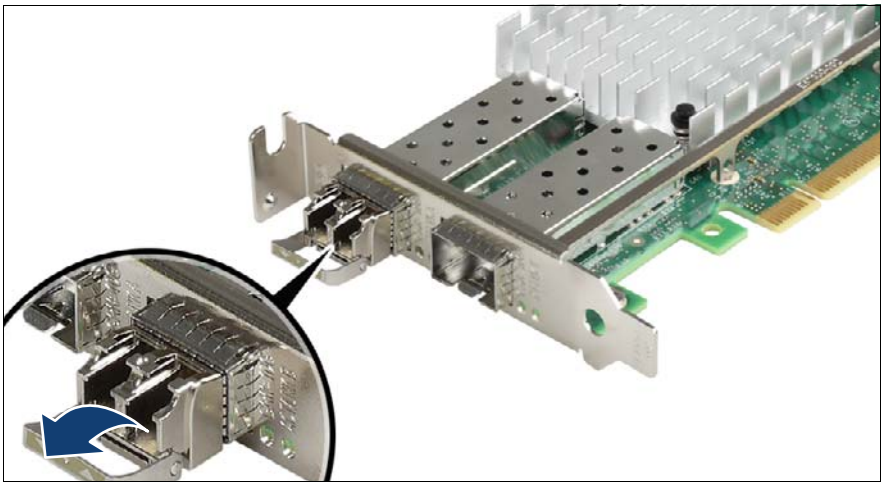


Figure 99: Unlatching the locking bail

► Carefully unlatch and fold down the locking bail on the SFP+ transceiver module to eject the transceiver from the socket connector.

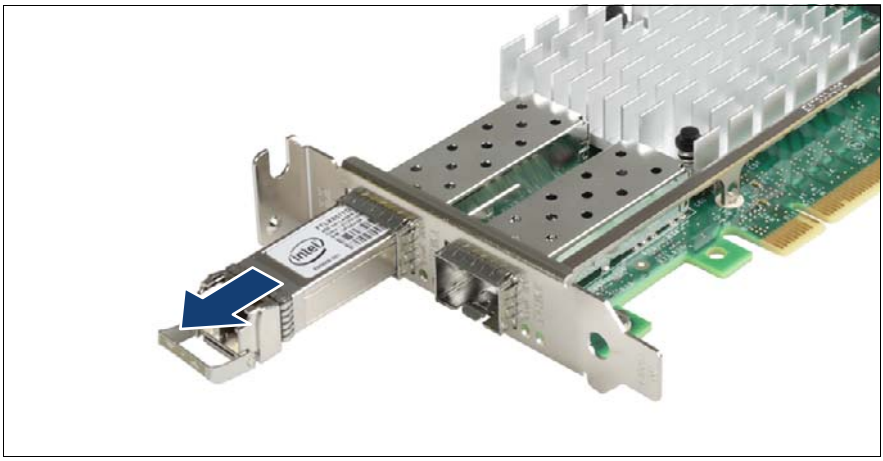


Figure 100: Removing the SFP+ transceiver

► Pull the SFP+ transceiver module out of its socket connector.

► Reattach the protective optical port plug to the transceiver optical bores.

Place the removed SFP+ transceiver module in an antistatic bag or other protective environment.

9.6.3 Replacing SFP+ transceiver modules

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tool:	tool-less

For Fiber Channel over Ethernet (FCoE) configurations, the ethernet server adapter is equipped with one or two SFP+ (small form-factor pluggable) transceiver modules.

Removing SFP+ transceiver modules

- Remove the defective SFP+ transceiver module(s) as described in section "Removing an SFP+ transceiver module" on page 190.

Installing SFP+ transceiver modules

- Unpack the new SFP+ transceiver module.
- Verify that the new SFP+ transceiver module is the same type of transceiver you are replacing.
- Install the new SFP+ transceiver module(s) as described in section "Installing SFP+ transceiver modules" on page 186.
- Inform the customer about changed WWN and MAC addresses. For further information, refer to section "Looking up changed MAC / WWN addresses" on page 89.

10 Main memory

Safety notes

CAUTION!

- Do not install unsupported third party memory modules. For further information on supported memory modules, refer to section "Basic information" on page 196.
- Memory modules remain hot after shutdown. Wait for components to cool down before installing or removing memory modules to prevent burns.
- Do not insert and remove memory modules repeatedly. Doing so may cause failures.
- Pressing out the securing clips on the memory slot will eject the installed memory module. To prevent damage and injuries eject memory modules carefully without applying excessive force.
- For further information, please refer to chapter "Important information" on page 35.

10.1 Basic information

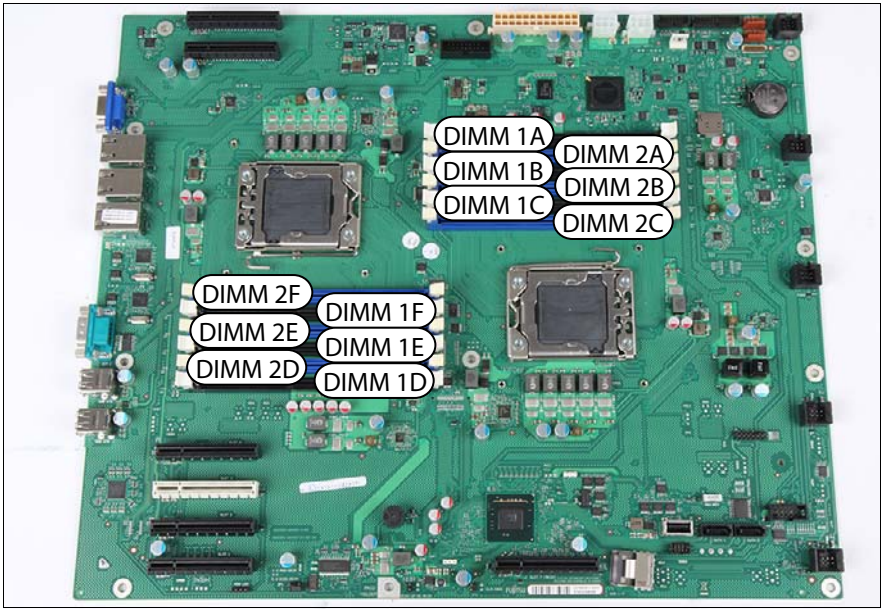


Figure 101: Memory overview

– The system board is equipped with 12 memory slots (6 connectors per CPU).
– In mono processor configurations only 6 memory slots are usable.
– The system has to be equipped with at least one memory module per processor.
– Supported capacities: 2 GB, 4 GB, 8 GB or16 GB
– Maximum amount of RAM: 192 GB (96 GB per CPU)
– Supported memory modules:

Type		Ranking[1]			Error Correction
		SR	DR	QR	
DDR3-1600 PC3-12800	RDIMMs (Registered DIMMs)	x	x	x	ECC

[1] SR: Single-Rank, DR: Dual-Rank, QR: Quad-Rank

10.1.1 Memory sequence

10.1.1.1 Population rules

– Populate memory slot 1 / channel A (DIMM 1A) first.

– In case of dual processor configurations, populate memory slot 1 / channel D (DIMM 1D) second.

– Within all channels, memory slot 1 must be populated prior to slot 2. (for all CPUs).

– If memory modules with different ranks are used, always populate the higher number rank DIMM first (starting from slot 1).

– If memory modules with different capacities are used:

  – Populate modules with higher capacities first.
  – Within a channel, populate modules in descending order of capacity.

– If memory modules with different speeds are used, the lowest clock rate applies for all DIMMs.

  Regardless of the mode, all DIMMs will run at the highest common frequency that is allowed by the SPD Data of the DIMMs and the maximum speed of the selected configuration.

– RDIMMs are allowed.

– Only ECC DIMMs are allowed.

– Mixing of quad-rank DIMMs in one channel and three DIMMs in another channel (3DPC) on the same CPU is not allowed.

10.1.1.2 Independant Channel mode

CPU	CPU1						CPU2					
Channel	A		B		C		D		E		F	
DIMM	1A	2A	1B	2B	1C	2C	1D	2D	1E	2E	1F	2F
#DIMMs	mono CPU configuration											
1	1											
2	1		2									
3	1		2		3							
4	1	4	2		3							
5	1	4	2	5	3							
6	1	4	2	5	3	6						
#DIMMs	dual CPU configuration											
2	1						2					
3	1		3				2					
4	1		3				2		4			
5	1		3		5		2		4			
6	1		3		5		2		4		6	
7	1	7	3		5		2		4		6	
8	1	7	3		5		2	8	4		6	
9	1	7	3	9	5		2	8	4		6	
10	1	7	3	9	5		2	8	4	10	6	
11	1	7	3	9	5	11	2	8	4	10	6	
12	1	7	3	9	5	11	2	8	4	10	6	12

10.1.1.3 Performance modes

CPU	CPU1						CPU2					
Channel	A		B		C		D		E		F	
DIMM	1A	2A	1B	2B	1C	2C	1D	2D	1E	2E	1F	2F
#DIMMs	mono CPU configuration											
3	1		1		1							
6	1	2	1	2	1	2						
#DIMMs	dual CPU configuration											
6	1		1		1		2		2		2	
9	1	3	1	3	1	3	2		2		2	
12	1	3	1	3	1	3	2	4	2	4	2	4

Notes on Mirrored Channel and Performance modes

– Always populate memory modules in triples.

– Same numbers mean identical modules (capacity, rank).

10.2 Installing memory modules

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools: tool-less

10.2.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Disabling SVOM boot watchdog functionality" on page 66
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

10.2.2 Installing a memory module

- Identify the correct memory slot see section "Memory sequence" on page 197.

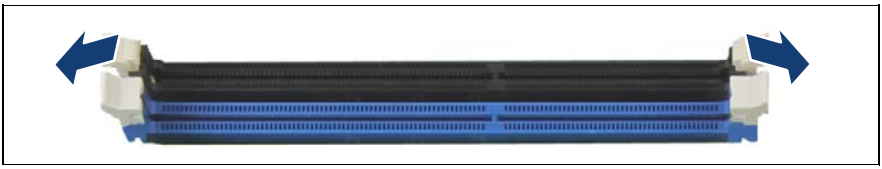


Figure 102: Installing memory modules (A)

- Press out the securing clip at each end of the memory slot.

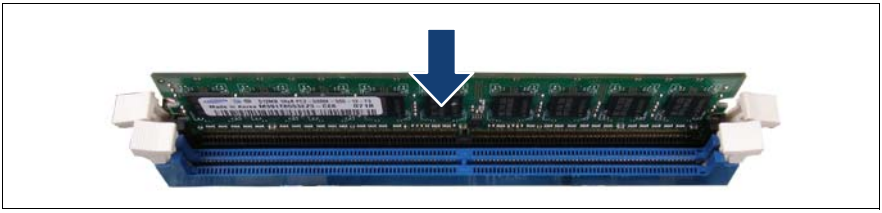


Figure 103: Installing memory modules (B)

- Align the notch on the bottom of the module with the crossbar in the slot.
- Press down on the memory module until the securing clips snap into the cutouts at each end of the module.

10.2.3 Concluding steps

- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- "Updating or recovering the system board BIOS and iRMC" on page 73
- "Enabling SVOM boot watchdog functionality" on page 82
- "Verifying the memory mode" on page 83
- "Enabling BitLocker functionality" on page 88

10.3 Removing memory modules

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools: tool-less

10.3.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Disabling SVOM boot watchdog functionality" on page 66
- "Locating the defective server" on page 47
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

10.3.2 Removing a memory module

- Identify the desired memory slot see section "Memory sequence" on page 197.

CAUTION!

Ensure to maintain an operational configuration when removing memory modules. For additional information, please refer to section "Basic information" on page 196.

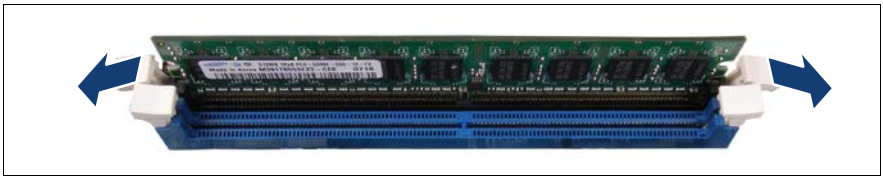


Figure 104: Removing memory modules (A)

- Eject the desired memory module by pressing out the securing clips at each end of the memory slot.

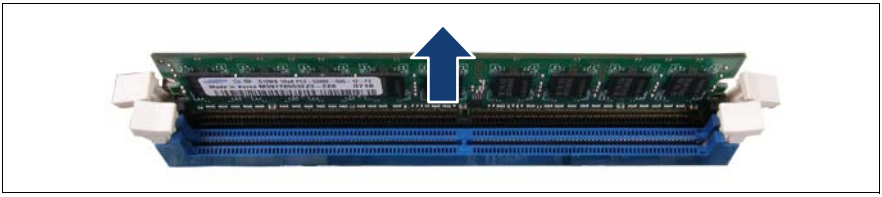


Figure 105: Removing memory modules (B)

► Remove the ejected memory module.

10.3.3 Concluding steps

► "Reassembling" on page 57
► "Connecting the server to the power source" on page 62
► "Updating or recovering the system board BIOS and iRMC" on page 73
► "Switching on the server" on page 64
► "Enabling SVOM boot watchdog functionality" on page 82
► "Enabling BitLocker functionality" on page 88

10.4 Replacing memory modules

Upgrade and Repair Unit (URU)

Hardware: 5 minutes
Software: 5 minutes

Tools:	tool-less

10.4.1 Preliminary steps

► "Locating the defective server" on page 47
► Identify the defective memory slot using the server management software.
► "Disabling BitLocker functionality" on page 65
► "Disabling SVOM boot watchdog functionality" on page 66

- "Shutting down the server" on page 49.
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

10.4.2 Removing the defective memory module

- Remove the defective memory module as described in section "Removing a memory module" on page 201.

10.4.3 Installing a new memory module

- Install memory module as described in section "Installing a memory module" on page 199.

10.4.4 Concluding steps

- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Updating or recovering the system board BIOS and iRMC" on page 73
- "Switching on the server" on page 64
- "Enabling SVOM boot watchdog functionality" on page 82
- "Enabling replaced components in the system BIOS" on page 82
- "Verifying the memory mode" on page 83
- "Enabling BitLocker functionality" on page 88

11 Processors

Safety notes

CAUTION!

- Do not install unsupported processors. For further information on supported processors, refer to section "Basic information" on page 206.
- Circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. Always discharge static build-up (e.g. by touching a grounded object) before handling electrostatic-sensitive devices (ESDs)
- Do not touch the circuitry on boards or soldered parts. Hold circuit boards by their metallic areas or edges.
- When removing or installing processors, be careful not to touch or bend the spring contacts on the processor sockets.
- Never touch the underside of the processors. Even minor soiling such as grease from the skin can impair the processor's operation or destroy the processors.
- For further information, please refer to chapter "Important information" on page 35.

11.1 Basic information

The system board D3169 offers two sockets for Intel Xeon processors.

11.1.1 Supported processors

– Intel Xeon E5-2500 processor series CPUs
– Socket type: LGA 2011 package
– Thermal Design Power (TDP) class: up to 95 W

11.1.2 Processor locations

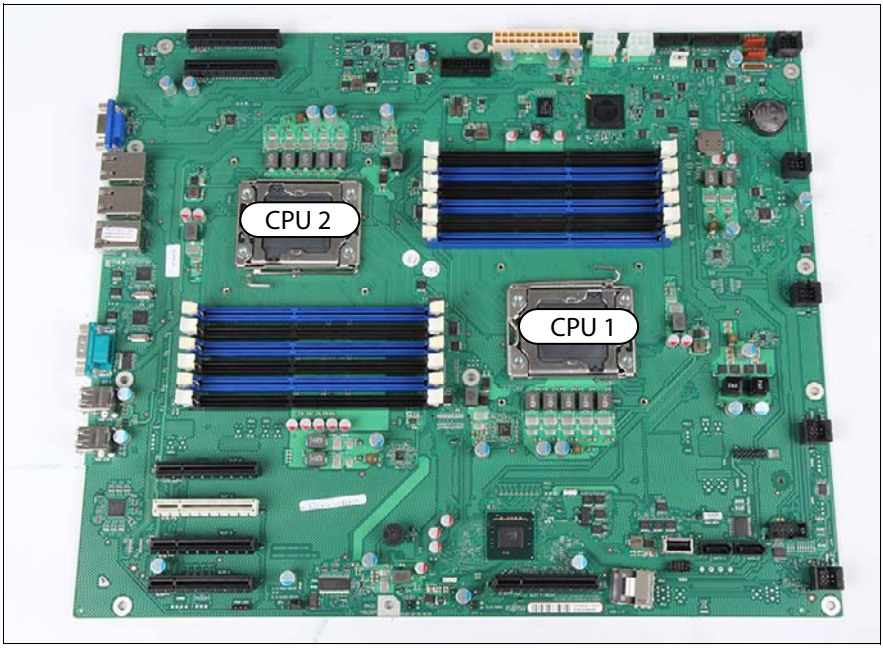


Figure 106: CPU locations on system board D3169

11.2 Installing processors

Upgrade and Repair Unit (URU)

Hardware: 15 minutes
Software: 5 minutes

Tool:	Phillips PH2 / (+) No. 2 screw driver

CAUTION!

Processors are extremely sensitive to electrostatic discharge and must be handled with care. After a processor has been removed from its protective sleeve or from its socket, place it upside down on a nonconducting, antistatic surface. Never push a processor over a surface.

11.2.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Disabling SVOM boot watchdog functionality" on page 66
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51.c

11.2.2 Installing the processor

This description applies to the following procedures:

– Installing the second CPU in a mono-processor configuration

– Transfering a CPU after replacing the system board (see section "Swapping processors" on page 327)

11.2.2.1 Removing the protective cover

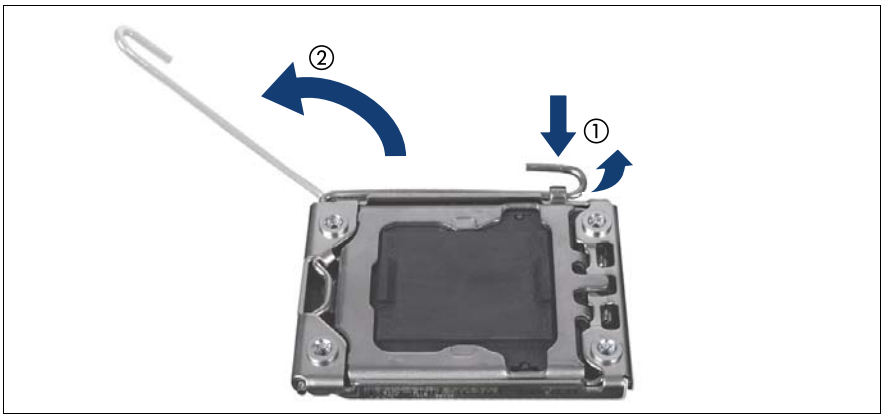


Figure 107: Opening socket release lever

► Unlatch the socket release lever by pushing it down and away from the socket (1) and then swivel it up (2)K

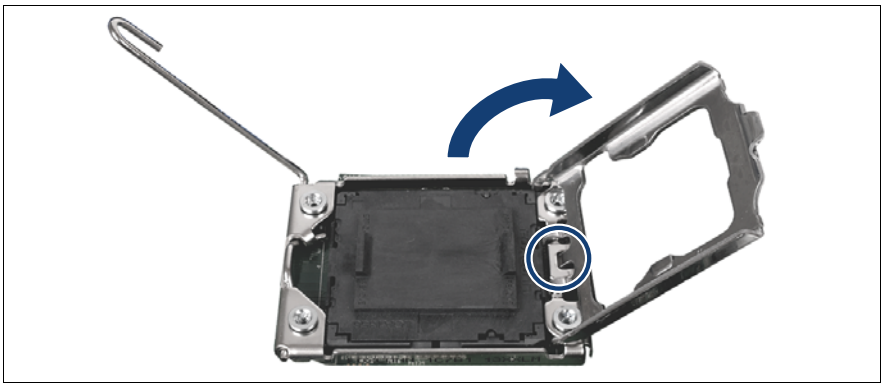


Figure 108: Opening the load plate

► Open the load plate of the processor socket.

CAUTION!

Handle the locking frame carefully.
In a vertical position, the small clip (see circle) can scratch the system board.

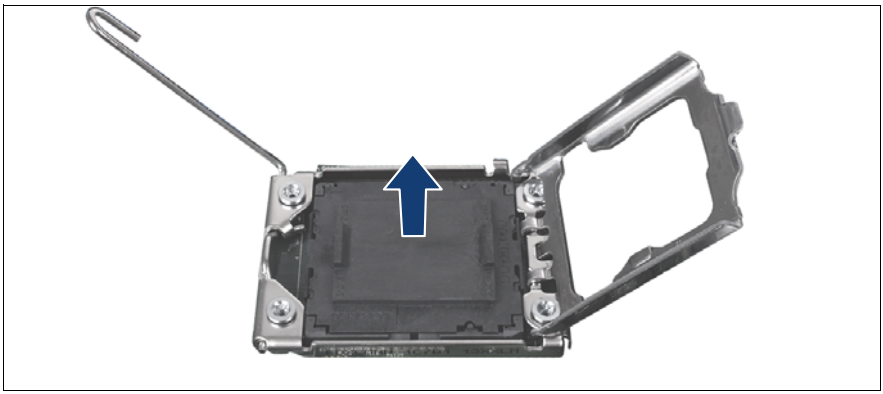


Figure 109: Removing the protective cover

► Remove the black protective cover from the processor socket.

11.2.2.2 Installing the new processor

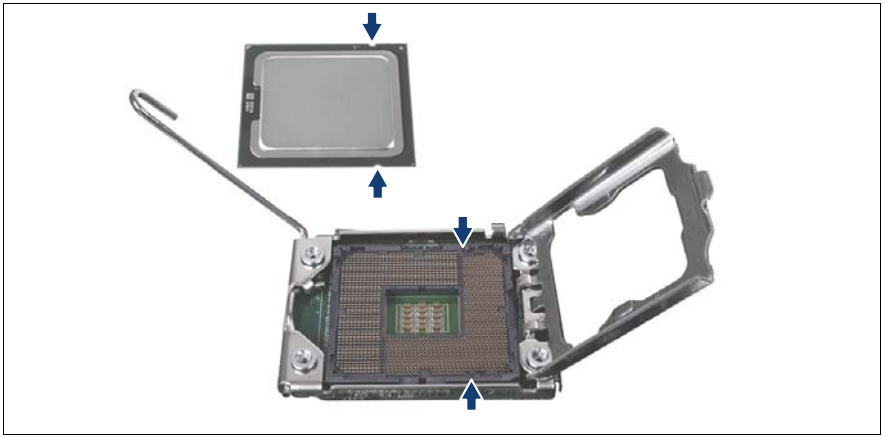


Figure 110: Installing the processor

Notice the coding!

► Hold the processor with your thumb and index finger.

► Place the new processor on the socket.

Make sure that the recesses on the processor are aligned with the corresponding markings on the socket.

CAUTION!

– Ensure that the processor is level in the socket.

– Be careful not to touch or bend the pins on the processor socket.

– Never touch the underside of the processor. Even minor soiling such as grease from the skin can impair the processor's operation or destroy the processor.

– Ensure not to scrape or dent the processor edges.

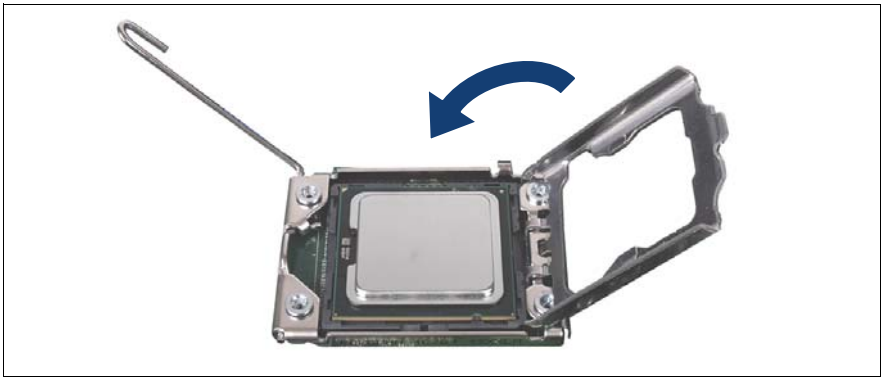


Figure 111: Closing the load plate

► Close the load plate of the processor.

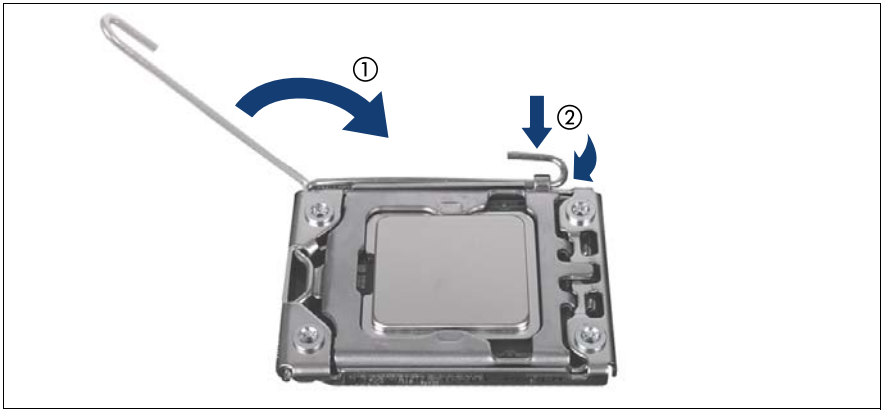


Figure 112: Closing the socket release lever

- Close the socket release lever (1) and latch it under the load plate retention tab (2) to lock down the load plate.
- If applicable, install the second processor accordingly.

11.2.3 Concluding steps

- "Installing processor heat sinks" on page 219
- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Updating or recovering the system board BIOS and iRMC" on page 73
- "Switching on the server" on page 64
- "Enabling SVOM boot watchdog functionality" on page 82
- "Enabling BitLocker functionality" on page 88

11.3 Removing processors

Upgrade and Repair Unit (URU)

Hardware: 15 minutes
Software: 5 minutes

Tool:	Phillips PH2 / (+) No. 2 screw driver

11.3.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Disabling SVOM boot watchdog functionality" on page 66
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51
- "Removing processor heat sinks" on page 222

11.3.2 Removing a processor

This description applies to the following procedures:

- Removing the second processor (CPU 2) from a dual-processor configuration
- Removing processors from a defective system board (see section "Removing a processor" on page 212)

- Remove the desired processor heat sink as described in section "Removing processor heat sinks" on page 222.

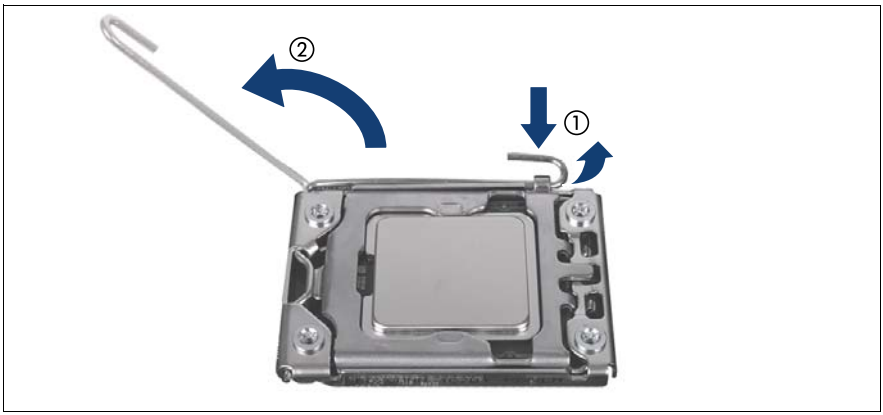


Figure 113: Opening socket release lever

► Unlatch the socket release lever by pushing it down and away from the socket (1) and then swivel it up (2).

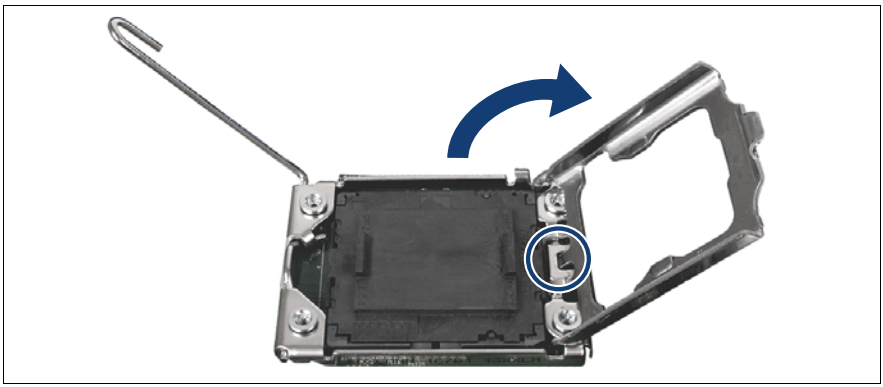


Figure 114: Opening the load plate

► Open the load plate of the processor socket.

CAUTION!

Handle the locking frame carefully.
In a vertical position, the small clip (see circle) can scratch the system board.

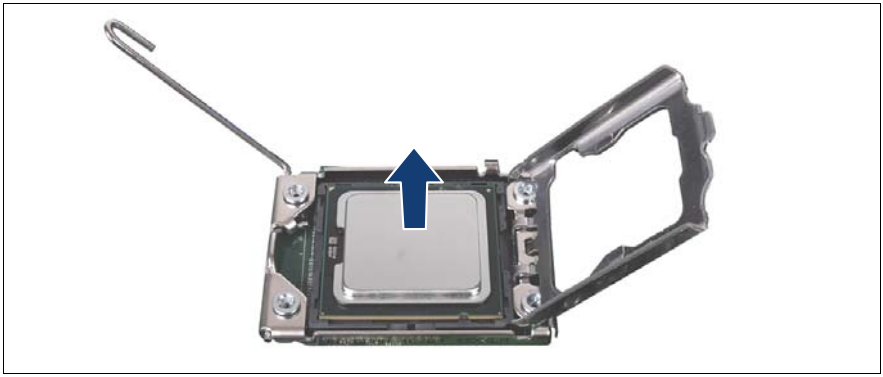


Figure 115: Removing the processor

► Carefully remove the defective processor from its socket in a vertical motion.

CAUTION!

Be careful not to touch or bend the spring contacts on the processor socket.

► Thoroughly clean residual thermal paste from the processor surface using a lint-free cloth.

► Store the processor in a save place for later reuse.

CAUTION!

Processors are extremely sensitive to electrostatic discharge and must be handled with care. After a processor has been removed from its protective sleeve or from its socket, place it upside down on a nonconducting, antistatic surface. Never push a processor over a surface.

Be careful not to touch or bend the spring contacts on the processor socket.

11.3.2.1 Installing the protective cover

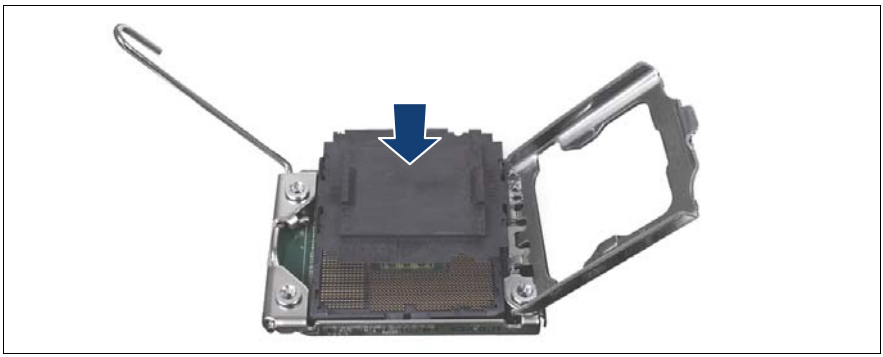


Figure 116: Attaching the protective socket cover

► Carefully lower the protective socket cover onto the processor socket in a vertical motion until it snaps in place.

Notice the coding!

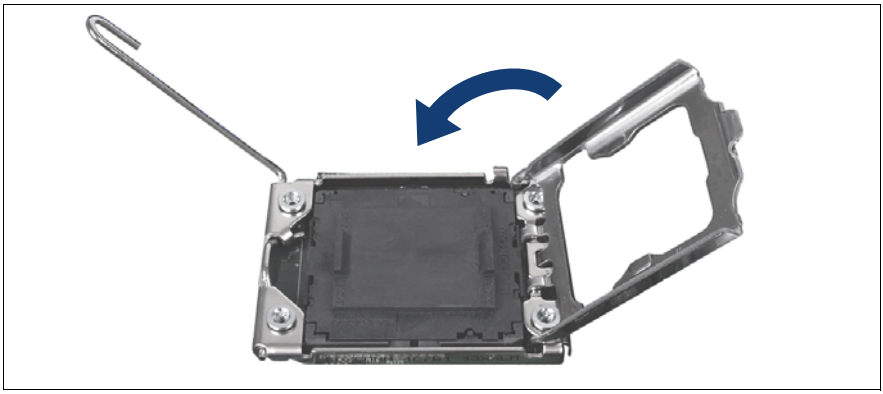


Figure 117: Closing the load plate

► Close the load plate of the processor.

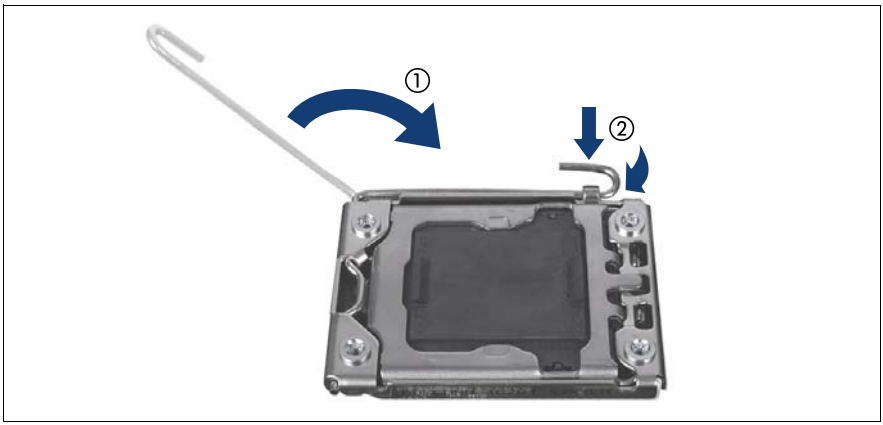


Figure 118: Close the socket release lever

► Close the socket release (1) lever and latch it under the load plate retention tab to lock down the load plate (2).

11.3.3 Concluding steps

► "Reassembling" on page 57

► "Connecting the server to the power source" on page 62

► If applicable, "Updating or recovering the system board BIOS and iRMC" on page 73

► "Switching on the server" on page 64

► "Enabling SVOM boot watchdog functionality" on page 82

► "Enabling BitLocker functionality" on page 88

11.4 Upgrading or replacing processors

Field Replaceable Unit (FRU)

Hardware: 15 minutes
Software: 5 minutes

Tool:	Phillips PH2 / (+) No. 2 screw driver

CAUTION!

Processors are extremely sensitive to electrostatic discharge and must be handled with care. After a processor has been removed from its protective sleeve or from its socket, place it upside down on a nonconducting, antistatic surface. Never push a processor over a surface.

11.4.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Disabling SVOM boot watchdog functionality" on page 66
- "Locating the defective server" on page 47
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51
- "Removing processor heat sinks" on page 222

11.4.2 Upgrading or replacing a processor

This description applies to the following procedures:

- Installing the second processor in a single-processor configuration
- Transfering a processor after replacing the system board (see section "Replacing the system board" on page 319)

- In case of installing a second processor remove the protective cover as described in section "Removing the protective cover" on page 208
- Remove the desired processor as described in section "Removing a processor" on page 212.
- Install the new processor as described in section "Installing the processor" on page 207.

11.4.3 Concluding steps

- "Installing processor heat sinks" on page 219

- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- If applicable, "Updating or recovering the system board BIOS and iRMC" on page 73
- "Switching on the server" on page 64
- "Enabling SVOM boot watchdog functionality" on page 82
- "Enabling BitLocker functionality" on page 88

11.5 Handling processor heat sinks

Field Replaceable Unit (FRU)
if thermal paste is involved

Hardware: 15 minutes

Upgrade and Repair Unit (URU)

Tool:	Phillips PH2 / (+) No. 2 screw driver

11.5.1 Preliminary steps

- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

11.5.2 Installing processor heat sinks

Figure 119: Standard processor heat sink V26898-B977-V101

11.5.2.1 Preparing the heat sink and processor

When installing a new heat sink

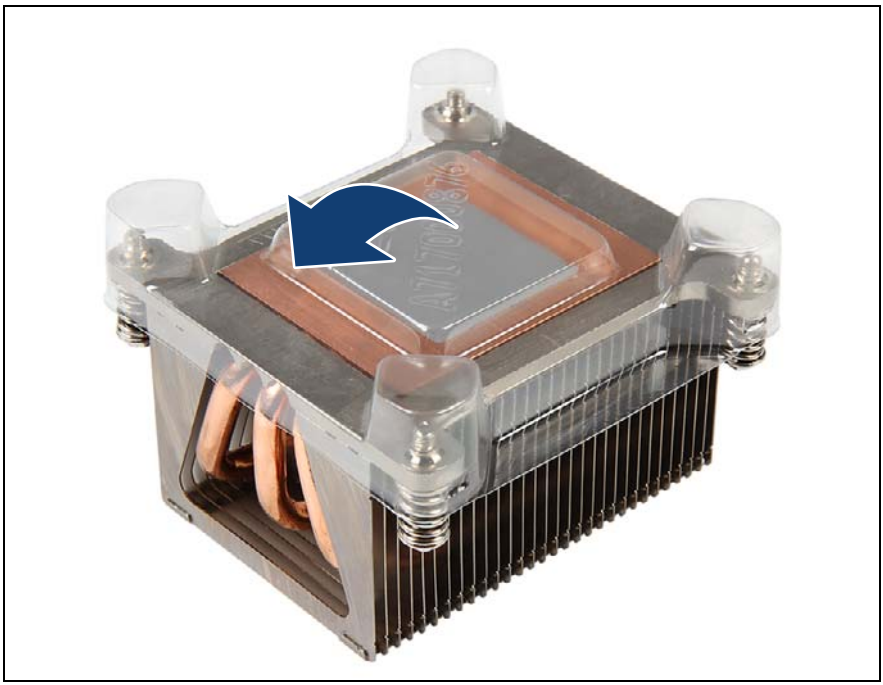


Figure 120: Removing the protective heat sink cover

- Remove the protective cover from the heat sink.

CAUTION!

Ensure not to touch the heat-conductive paste on the bottom of the heat sink.

When reusing a heat sink

- Ensure that all residual thermal paste has been thoroughly cleaned off the copper surface of the heat sink.
- Apply thermal paste to the processor surface as described in section "Applying thermal paste" on page 225.

11.5.2.2 Installing the heat sink

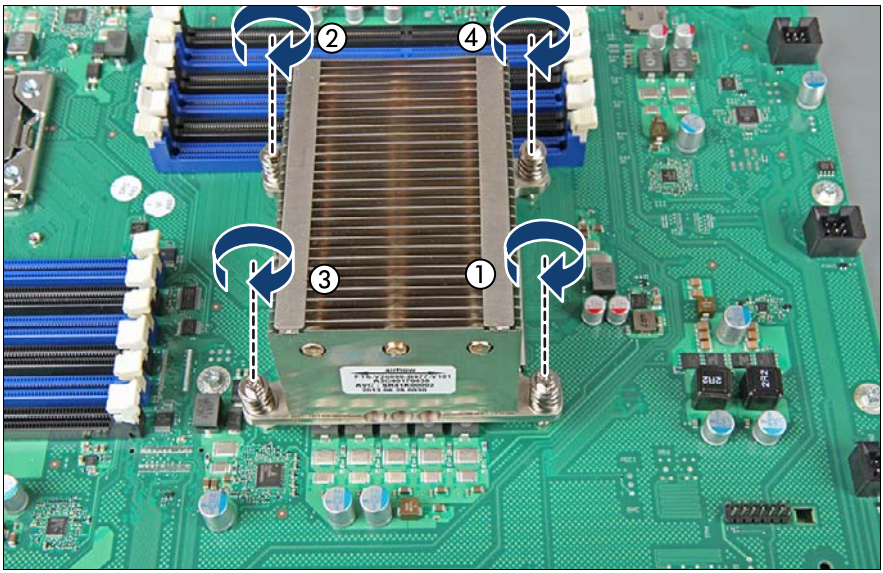


Figure 121: Installing the heat sink

- ► Align the heat sink with the uncovered copper heat pipes (H, see above) facing towards the PSU.
- ► Carefully seat the heat sink on the four threaded holes as shown (see close-up).

CAUTION!

– Ensure that the screws on the heat sink are properly seated on the threaded holes.

– Ensure that the heat sink cooling fins match the direction of the airflow!

- ► Fasten the four captive screws on the heat sink in a crossover pattern (screw torque: 1.0 Nm, not applicable for the Japanese market) (1-4).

11.5.3 Removing processor heat sinks

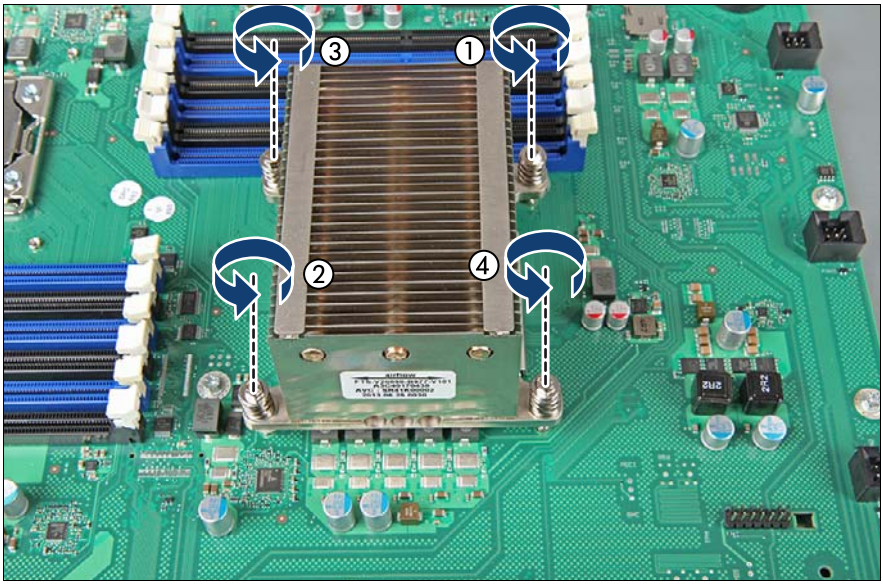


Figure 122: Removing the processor heat sink (A)

► Loosen the four captive screws on the heat sink in a crossover pattern (1-4).

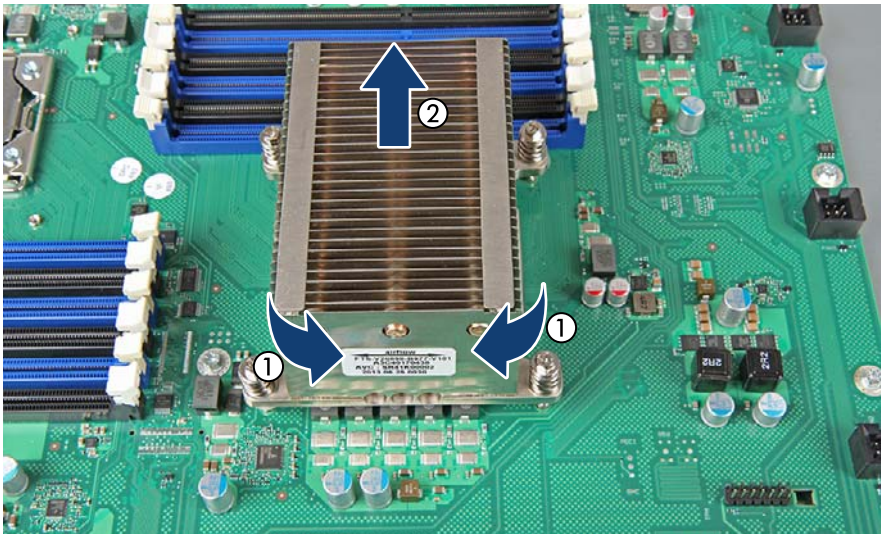


Figure 123: Removing the processor heat sink (B)

► Carefully turn the heat sink back and forth to detach it from the processor (1).

This may be necessary due to the adhesive quality of the thermal paste located between the heat sink and processor.

CAUTION!

Pay special attention not to damage any system board components surrounding the processor socket.

► Lift the heat sink out of the chassis (2).

► Thoroughly clean residual thermal paste from the surface of the heat sink and the processor using a lint-free cloth.

11.5.4 Replacing processor heat sinks

11.5.4.1 Removing the processor heat sink

► Remove the processor heat sink as described in section "Removing processor heat sinks" on page 222.

11.5.4.2 Applying thermal paste

► Apply thermal paste to the processor surface as described in section "Applying thermal paste" on page 225.

> If the processor upgrade or replacement kit contains a new CPU heat sink, a thin layer of thermal compound has already been pre-applied to its lower surface. In this case, please proceed with section "Installing the heat sink" on page 221.

11.5.4.3 Installing the processor heat sink

► Install the processor heat sink as described in sections "Preparing the heat sink and processor" on page 220 and "Installing the heat sink" on page 221.

11.5.5 Concluding steps

► "Reassembling" on page 57

► "Connecting the server to the power source" on page 62

► "Switching on the server" on page 64

11.6 Applying thermal paste

Field Replaceable Unit (FRU)

Hardware: 5 minutes

Tool:	tool-less

– For the Japanese market, the service engineer must follow the instruction provided separately.

– If the processor upgrade or replacement kit contains a new CPU heat sink, a thin layer of thermal compound has already been pre-applied to its lower surface. In this case, please proceed with section "Installing processor heat sinks" on page 219.

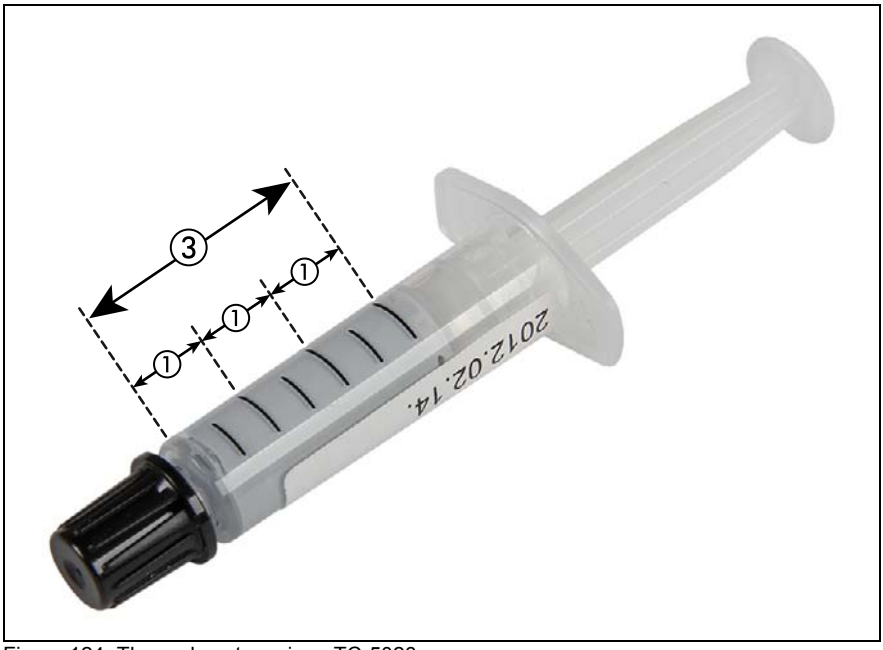


Figure 124: Thermal paste syringe TC-5026

One thermal compound syringe (A3C40142460 / 34035576) contains thermal paste for three processors.

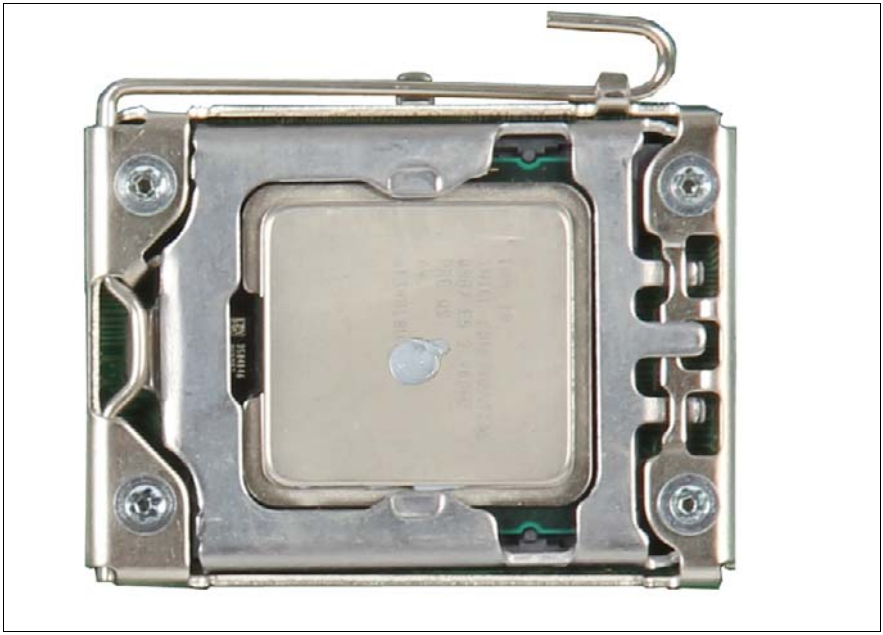


Figure 125: Applying thermal paste

► Apply a dot of thermal paste to the center of the processor surface as shown.

Two graduation marks on the syringe equal the correct amount of thermal paste for one processor.

CAUTION!

Do not mix different types of thermal paste.

12 Accessible drives

Safety notes

CAUTION!

- Before installing an accessible drive, acquaint yourself with the drive's user documentation.
- When inserting an accessible drive into the server, ensure not to pinch or strain any connected cables.
- When installing an accessible drive, hold it by its sides. Applying force to the top of the casing may cause failures.
- When disposing of, transferring, or returning a backup drive, ensure that all backup media has been removed from the drive.
- Do not touch the circuitry on boards or soldered parts. Hold circuit boards by their metallic areas or edges.
- Circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. Always discharge static build-up (e.g. by touching a grounded object) before handling electrostatic-sensitive devices (ESDs).
- For further safety information, please refer to chapter "Important information" on page 35.

12.1 Basic informations

Mounting order for accessible drives in the front panel cage

PRIMERGY RX2520 M1 server offers one 5.25-inch accessible drive bays for optical disk drives and backup drives:

Figure 126: Accessible drives in front panel cage

No.	Accessible drive	Bay	Max. no.
1	Local Service Display	3.5-inch bay	1
2	Optical disk drive	5.25 inch bay	1

Mounting order for accessible drives in the HDD bays

PRIMERGY RX2520 M1 server offers several possibilities to install tape drives:

Figure 127: Accessible drive (LTO) in HDD bays for 2.5-in HDD version

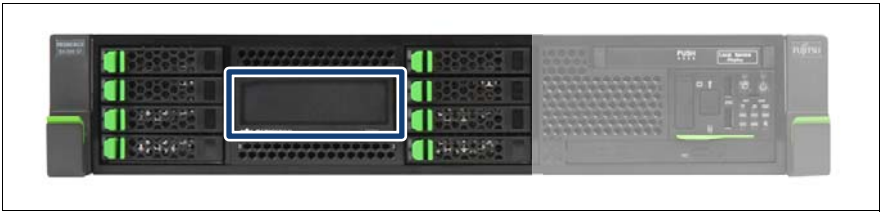


Figure 128: Accessible drive (RDX) in HDD bay for 2.5-in HDD version

12.2 Installing a Local Service Display (LSD) module

Upgrade and Repair Unit (URU)

Hardware: 10 minutes

Tools: tool-less

12.2.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51
- "Removing the fan box" on page 144

12.2.2 Removing the LSD dummy cover

Figure 129: Removing the LSD dummy cover

► Take the LSD dummy cover by the two recessed grips and pull out the LSD dummy cover.

CAUTION!

Save the LSD dummy cover for future use.
Always replace dummy covers into unused drive bays to comply with applicable EMC regulations and satisfy cooling requirements.

12.2.3 Installing a LSD module

Figure 130: Installing the LSD module

► Insert the LSD module into the bay and push in until it locks in place.

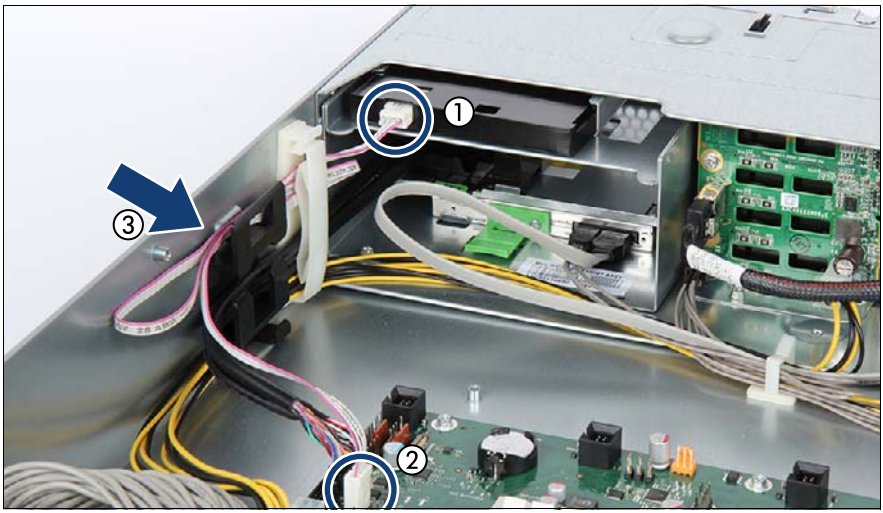


Figure 131: Installing the LSD module

► Connect the LSD cable to the LSD module (1).

► Connect the LSD cable to the connector SMB1 of the system board (2).

► Route the LSD cable through the upper cable guide (3).

12.2.4 Concluding steps

- "Installing the fan box" on page 146
- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Enabling BitLocker functionality" on page 88

12.3 Removing a LSD module

Upgrade and Repair Unit (URU)

Hardware: 10 minutes

Tools: tool-less

12.3.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51
- "Removing the fan box" on page 144

12.3.2 Removing the LSD module

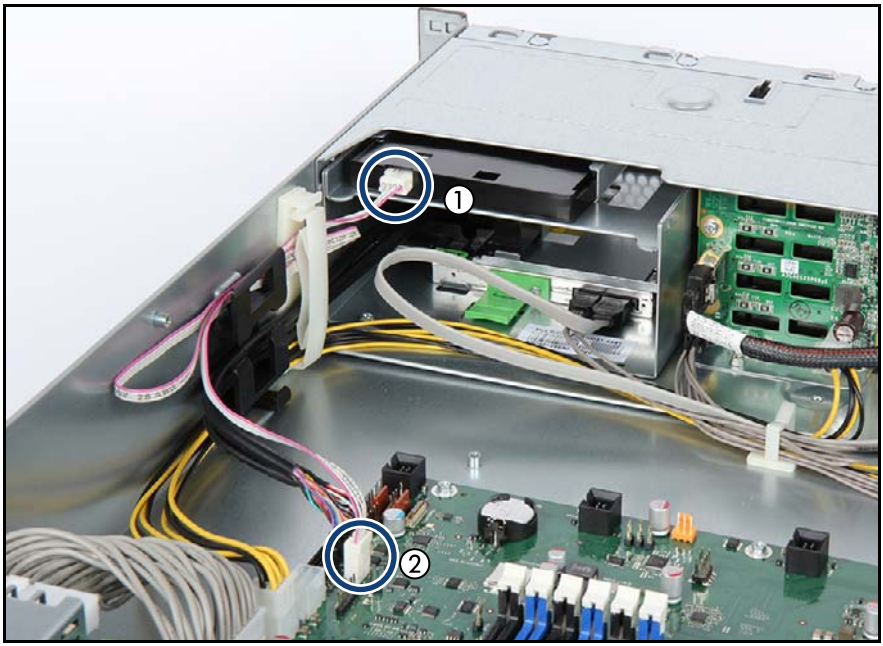


Figure 132: Removing the LSD cable

► Remove the LSD cable from the LSD module (1) and the connector on the system board (2).

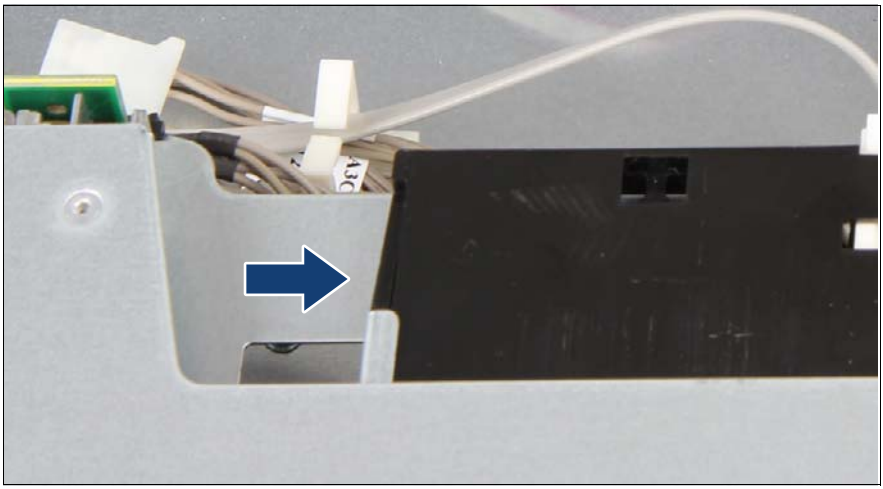


Figure 133: Unlocking the LSD module

► Press in on the locking latch to disengage the LSD module.

Figure 134: Unlocking the LSD module

► Pull the LSD module out of the bay.

Figure 135: Insert the LSD dummy cover

► Insert the LSD dummy cover into the bay.

12.3.3 Concluding steps

► "Installing the fan box" on page 146

► "Reassembling" on page 57

► "Connecting the server to the power source" on page 62

► "Enabling BitLocker functionality" on page 88

12.4 Replacing a LSD module

Upgrade and Repair Unit (URU)

Hardware: 10 minutes

Tools: tool-less

12.4.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51
- "Removing the fan box" on page 144

12.4.2 Removing the defective LSD module

- "Removing the LSD module" on page 233

12.4.3 Installing the new LSD module

- "Installing a LSD module" on page 231

12.4.4 Concluding steps

- "Installing the fan box" on page 146
- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Enabling BitLocker functionality" on page 88

12.5 Installing the optical disk drive (ODD)

Upgrade and Repair Unit (URU)

Hardware: 10 minutes

Tools:	Phillips PH0 / (+) No. 0 screw driver

12.5.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51
- "Removing the fan box" on page 144

12.5.2 Removing the ODD dummy module

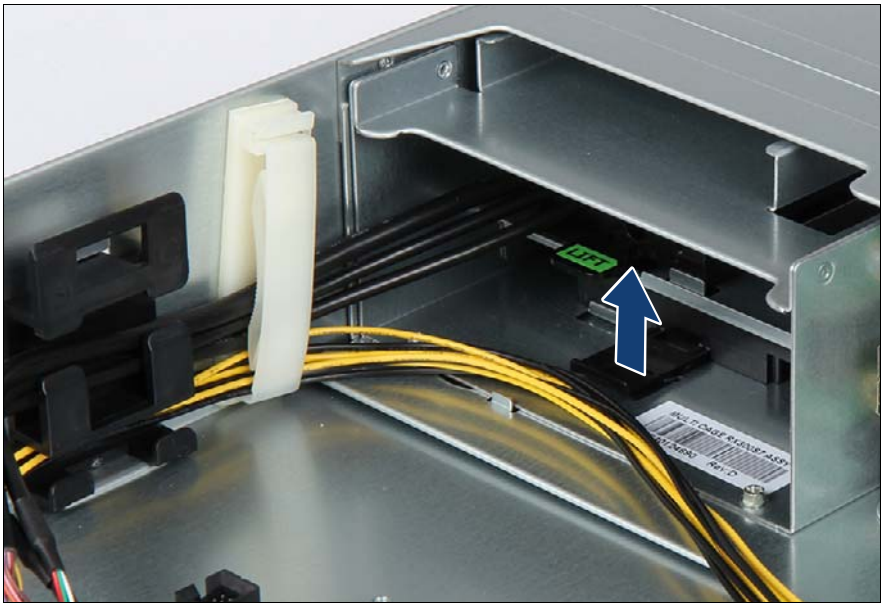


Figure 136: Removing the ODD dummy module

- Pull the locking latch upward to unlock the ODD dummy module.

CAUTION!

Save the ODD dummy module for future use.
Always replace dummy modules into unused drive bays to comply with applicable EMC regulations and satisfy cooling requirements.

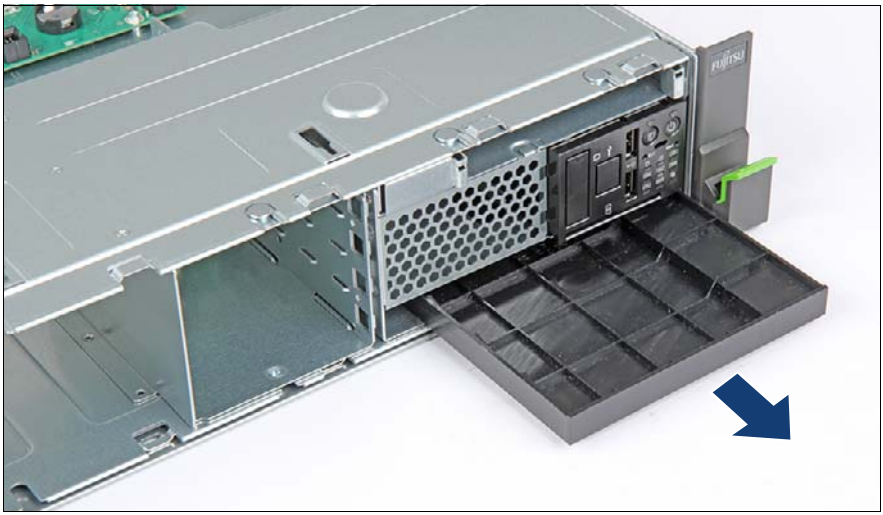


Figure 137: Removing the dummy module

► Pull the ODD dummy module out.

12.5.3 Preparing an ODD

Figure 138: Location for the unused ODD latch

► Take the ODD latch from its place on the bottom of the front panel module.

For the Japanese market: You can find the ODD latch in the delivered accessory kit.

Figure 139: Installing the ODD latch

► Mount the ODD latch to the ODD (1) and secure it with two screws (2).

12.5.4 Installing an ODD

Figure 140: Installing the ODD

► Insert the ODD into the bay and push in until it locks in place.

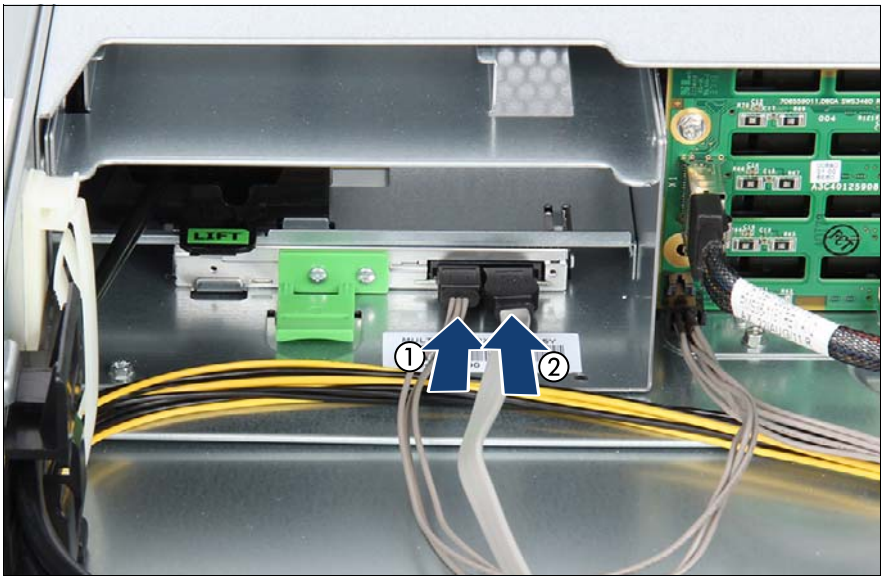


Figure 141: Installing the ODD

- Run the SATA and power cables through the ODD bay opening as shown.
- Connect the power cable to the ODD (1).
- Connect the SATA cable to the ODD (2).

12.5.5 Concluding steps

- "Installing the fan box" on page 146
- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Enabling BitLocker functionality" on page 88

12.6 Removing the optical disc drive (ODD)

Upgrade and Repair Unit (URU)

Hardware: 10 minutes

Tools:	Phillips PH0 / (+) No. 0 screw driver

12.6.1 Preliminary steps

- Ask the system administrator to eject all remaining backup or optical media from the backup or optical disk drive before removing it from the server.
- "Disabling BitLocker functionality" on page 65
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51
- "Removing the fan box" on page 144

12.6.2 Removing the ODD

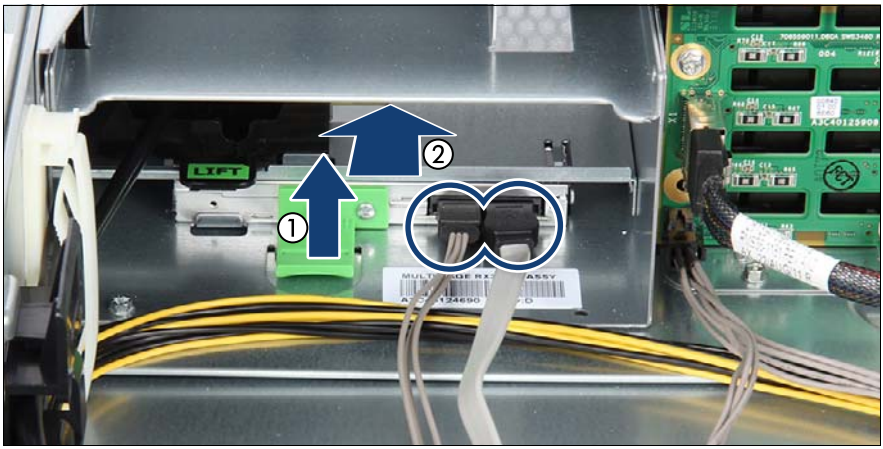


Figure 142: Removing the ODD (A)

- ► Disconnect the SATA cable (1) and the power cable (2).
- ► Pull the locking latch upward to unlock the ODD.
- ► Push the ODD out of the bay.

Figure 143: Removing the ODD latch

- ► Remove the two screws (1).
- ► Remove the ODD latch on the rear of the ODD (2).
- ► Fix the ODD latch in the bottom of the front panel module see figure 138 on page 238.

Figure 144: Installing the ODD dummy module

► Insert the ODD dummy module.

12.6.3 Concluding steps

► "Installing the fan box" on page 146

► "Reassembling" on page 57

► "Connecting the server to the power source" on page 62

► "Enabling BitLocker functionality" on page 88

12.7 Replacing an ODD

Upgrade and Repair Unit (URU)

Hardware: 10 minutes

Tools:	Phillips PH0 / (+) No. 0 screw driver

12.7.1 Preliminary steps

- Ask the system administrator to eject all remaining backup or optical media from the backup or optical disk drive before removing it from the server.
- "Disabling BitLocker functionality" on page 65
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51
- "Removing the fan box" on page 144

12.7.2 Removing the defective ODD

- "Removing the ODD" on page 242

12.7.3 Installing the new ODD

- "Preparing an ODD" on page 238
- "Installing an ODD" on page 240

12.7.4 Concluding steps

- "Installing the fan box" on page 146
- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Enabling BitLocker functionality" on page 88

12.8 Installing a RDX drive in 2.5-inch version

Notes on RDX drive USB cabling:

– A USB 2.0 RDX drive may be replaced by a USB 3.0 RDX drive with previous cabling.

– A USB 3.0 RDX drive may be connected with a USB 2.0 cable to an onboard USB 2.0 connector with limited performance.

– For full performance, connect the USB 3.0 RDX drive to a USB 3.0 interface card by USB 3.0 cable.

– The USB 3.0 cable cannot be connected to a USB 2.0 RDX drive.

– Connect the RDX drive to the onboard connector of the system board with cable C17.

– Connect the RDX drive to the USB 3.0 interface card with cable C22.

Upgrade and Repair Unit (URU)

Hardware: 10 minutes

Tools:	Phillips PH2 / (+) No. 2 screw driver

12.8.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Locating the defective server" on page 47
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51
- "Removing the fan box" on page 144

12.8.2 Installing a RDX drive in the cage

- Removing the 2.5-inch-HDD cage out of bay 1 and 2 for further information see section "Removing a HDD cage" on page 137.

Figure 145: Inserting the RDX drive in the drive cage

► Insert the RDX drive into the bay and push in.

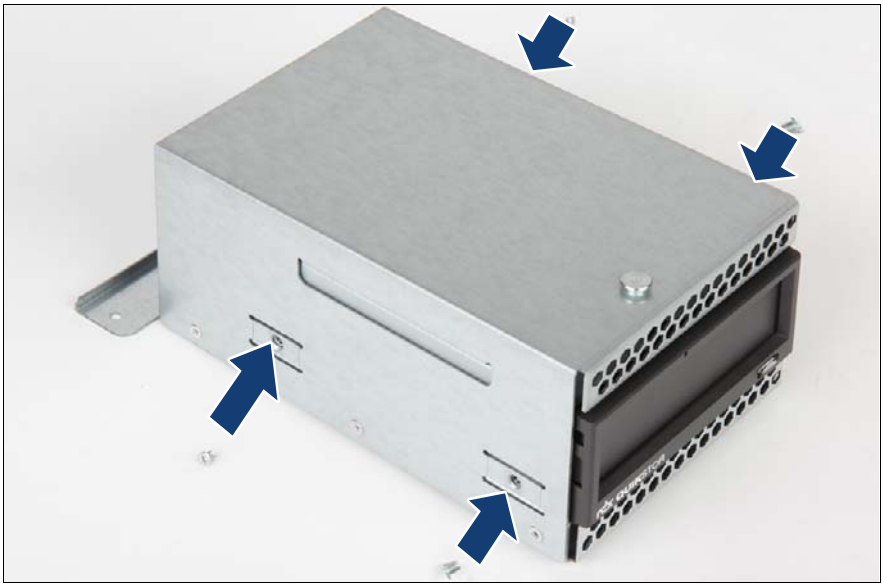


Figure 146: Fastening the RDX drive in the drive cage

► Fasten the RDX drive with 4 screws in the drive cage.

12.8.3 Installing the RDX drive

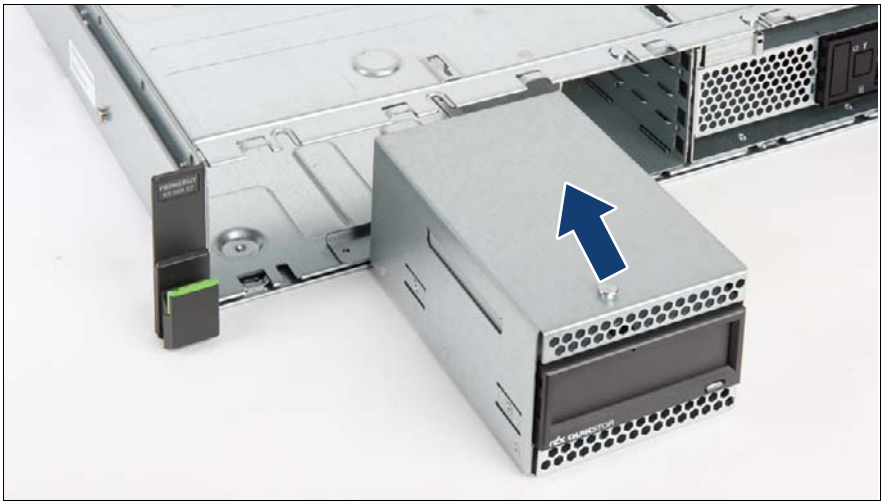


Figure 147: Installing the RDX drive

- ► Insert the RDX with the drive cage in the bay.
- ► Insert the HDD cage in bay1 see "Installing a HDD cage" on page 139.

12.8.4 Connecting the RDX drive

12.8.4.1 Connecting the RDX drive to the system board

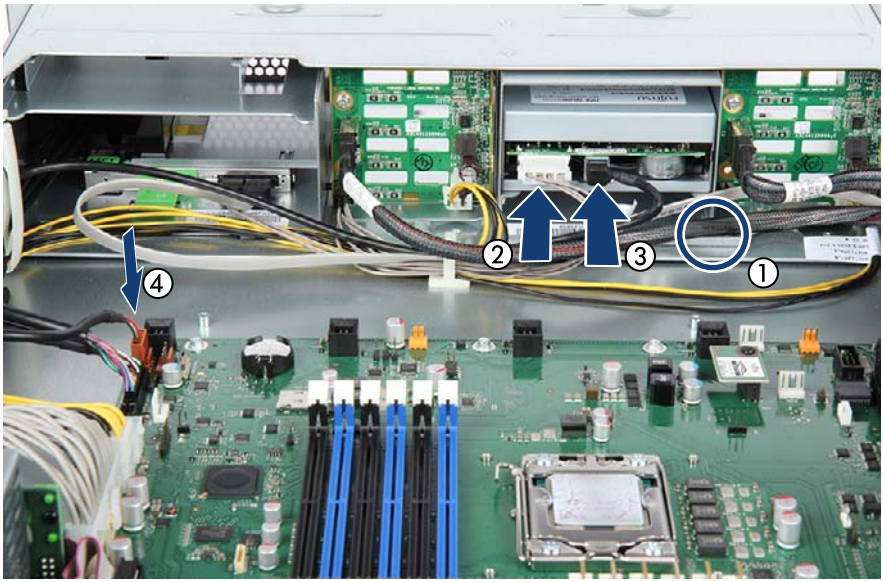


Figure 148: Connecting the cables to the RDX drive

- ► Fasten the drive cage with the screw (1).
- ► Connecting the power cable C5 to the RDX drive (2).
- ► Connecting the USB cable C17 to the RDX drive (3).
- ► Connect the USB cable C17 to the connector USB INT1 on the system board (4).
- ► Route the cables as shown.

12.8.4.2 Connecting the RDX drive to the USB 3.0 interface card

- ► Install the USB 3.0 interface card, see section "Installing a slot bracket to the USB 3.0 interface card D3305" on page 157 and section "Installing an expansion card" on page 160.

Figure 149: Installing the RDX drive cage

► Fasten the drive cage with the screw.

Figure 150: Connecting the USB cable to the USB 3.0 interface card

► Connecting the power cable C5 to the RDX drive (1).

► Connecting the USB cable C22 to the RDX drive (2).

► Route the cables as shown.

► Connect the USB cable C22 to the USB 3.0 interface card (3).

12.8.5 Concluding steps

- "Installing the fan box" on page 146
- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- "Verifying and configuring the backup software solution" on page 79
- "Enabling BitLocker functionality" on page 88

12.9 Removing a RDX drive in 2.5-inch version

Upgrade and Repair Unit (URU)

Hardware: 10 minutes

Tools: Phillips PH2 / (+) No. 2 screw driver

12.9.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Locating the defective server" on page 47
- "Removing backup and optical disk media" on page 69
- "Verifying and configuring the backup software solution" on page 69
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

12.9.2 Removing the drive cage

- Removing the 2.5-inch-HDD cage out of bay 1.

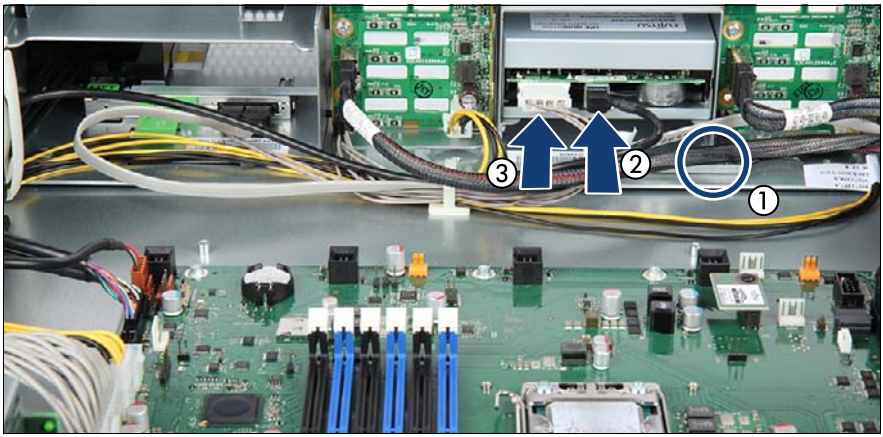


Figure 151: Removing the cables from the RDX drive

- ► Removing the screw that fasten the drive cage(1).
- ► Disconnecting the USB cable (2).
- ► Disconnecting the power cable (3).

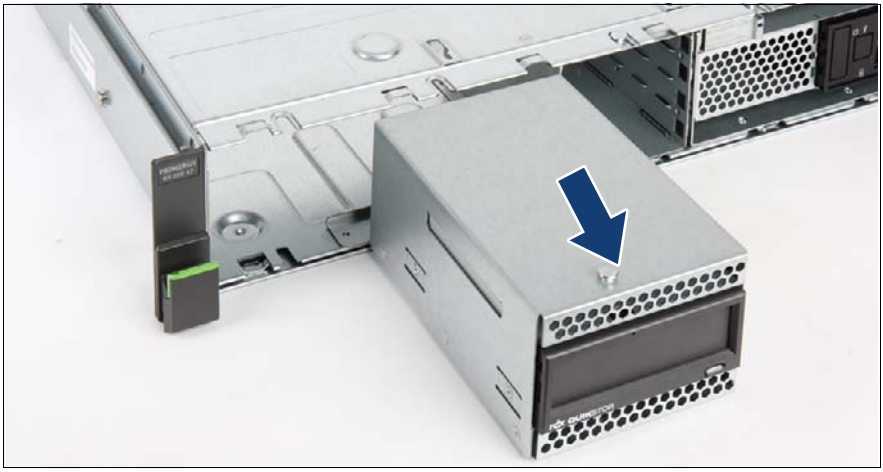


Figure 152: Unlocking the drive cage

- ► Remove the drive cage.

12.9.3 Removing a RDX drive out of the cage

Figure 153: Removing the 4 screws

► Remove the 4 screws from the drive cage

Figure 154: Installing tape drive dummy cover

► Insert the tape drive dummy cover into the drive cage.

Figure 155: Installing tape drive dummy module

- Fasten the tape drive dummy module with 2 screws.
- Insert the drive cage into bay 2, for further information see sectjon "Installing the RDX drive" on page 248.
- Insert the HDD cage into bay 1, for further information see sectjon "Installing a HDD cage" on page 139.
- If applicable, remove the USB 3.0 interface card as describe in section "Removing an expansion card" on page 165

12.9.4 Concluding steps

- "Installing the fan box" on page 146
- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- "Verifying and configuring the backup software solution" on page 79
- "Enabling BitLocker functionality" on page 88

12.10 Replacing the RDX drive in 2.5-inch version

Upgrade and Repair Unit (URU)

Hardware: 10 minutes

Tools: Phillips PH2 / (+) No. 2 screw driver

12.10.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Locating the defective server" on page 47
- "Removing backup and optical disk media" on page 69
- "Verifying and configuring the backup software solution" on page 69
- "Shutting down the server" on page 49

- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51
- "Removing the fan box" on page 144

12.10.2 Removing the defective RDX drive

- "Removing the drive cage" on page 251
- "Removing a RDX drive out of the cage" on page 253

12.10.3 Installing the new RDX drive

- "Installing a RDX drive in the cage" on page 246
- "Installing the RDX drive" on page 248

12.10.4 Concluding steps

- "Installing the fan box" on page 146
- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- "Verifying and configuring the backup software solution" on page 79
- "Enabling BitLocker functionality" on page 88

12.11 Installing an LTO drive in 2.5-inch version

Upgrade and Repair Unit (URU)

Hardware: 10 minutes

Tools:	Phillips PH2 / (+) No. 2 screw driver

12.11.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Locating the defective server" on page 47
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51
- "Removing the fan box" on page 144

12.11.2 Removing the drive cage

- Remove the screws on the rear side of the drive cage see also"Removing the drive cage" on page 264.

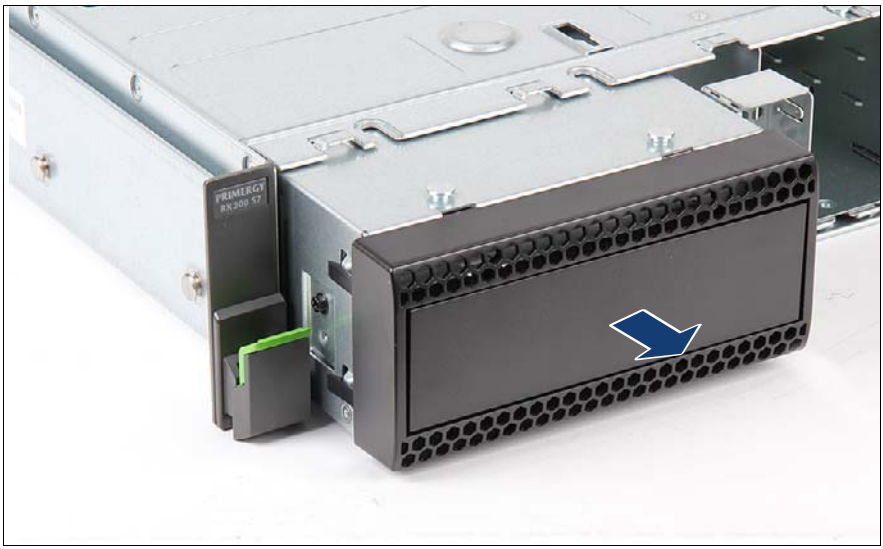


Figure 156: Removing the drive cage

- Push the LTO drive out of the bay.

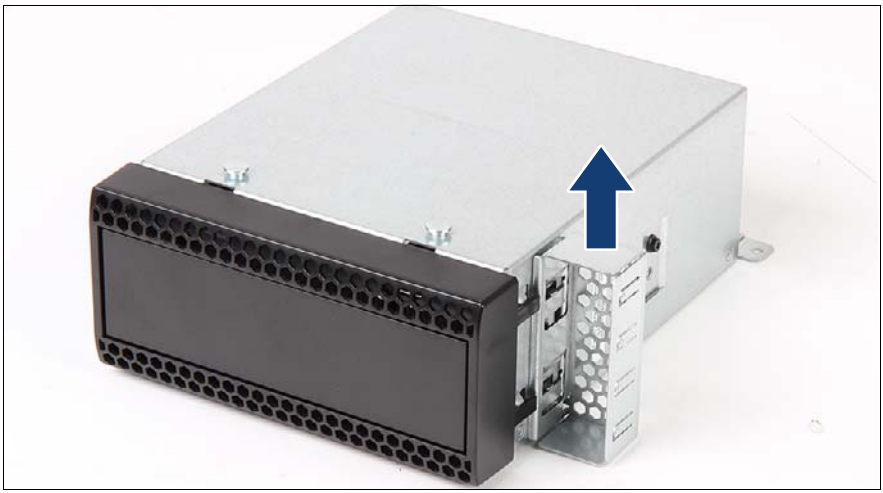


Figure 157: Removing the cover plate

► Remove the cover plate.

12.11.3 Removing the tape drive dummy module

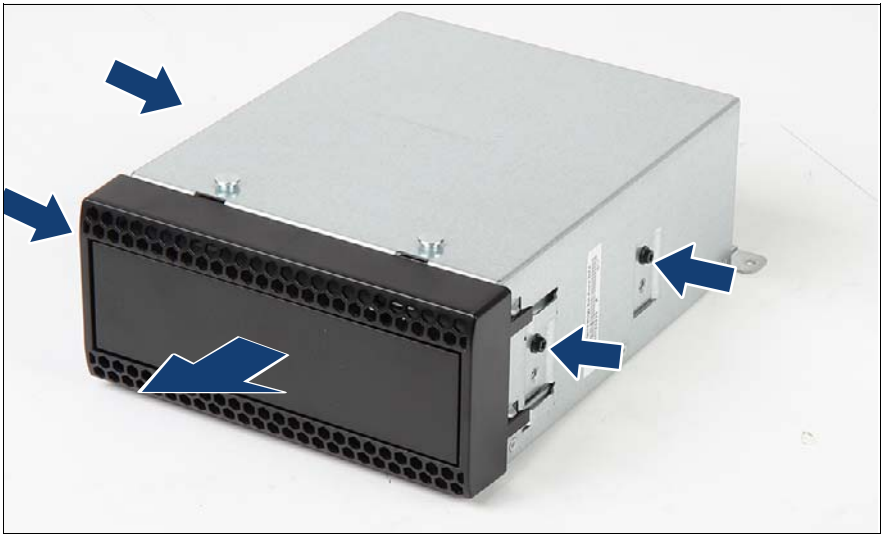


Figure 158: Removing the tape drive dummy module

- ► Remove the four screws.
- ► Pull out the tape drive dummy module.

12.11.4 Installing an LTO drive in the cage

Figure 159: Inserting the LTOdrive

- ► Insert the LTO drive into the bay and push in.

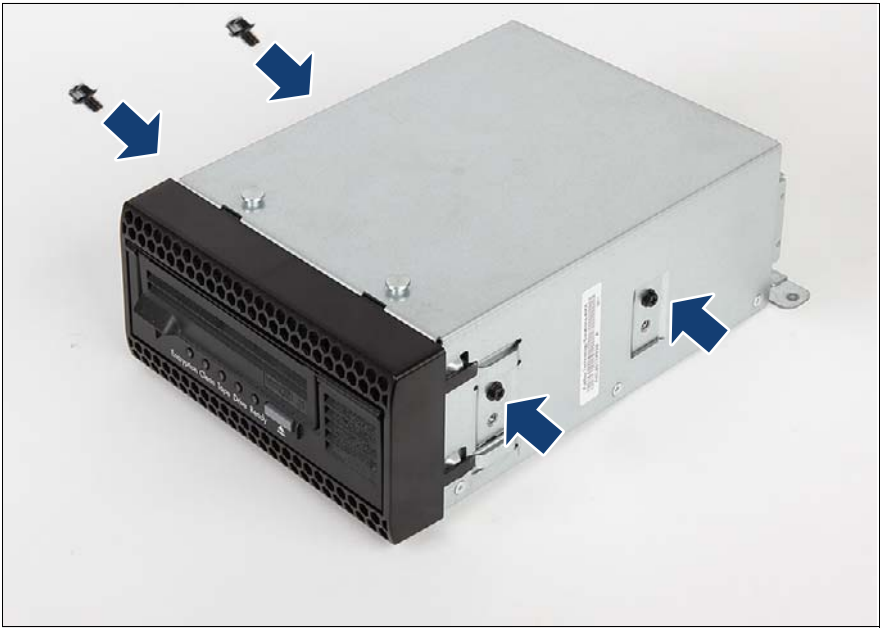


Figure 160: Fastening the LTO drive in the drive cage

► Fasten the LTO drive with 4 screws in the drive cage using the upper screw holes.

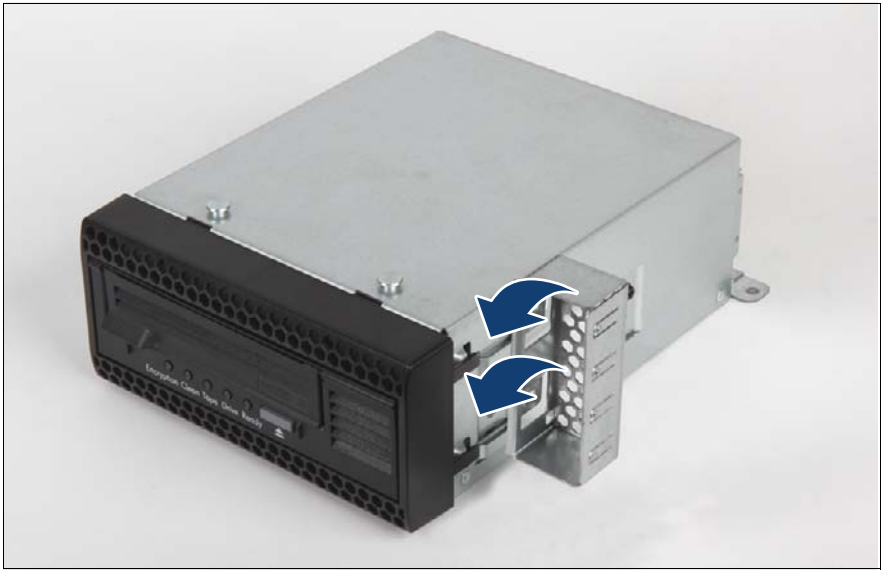


Figure 161: Connecting the cover plate

► Connect the cover plate to the LTO drive.

12.11.5 Installing the LTO cage

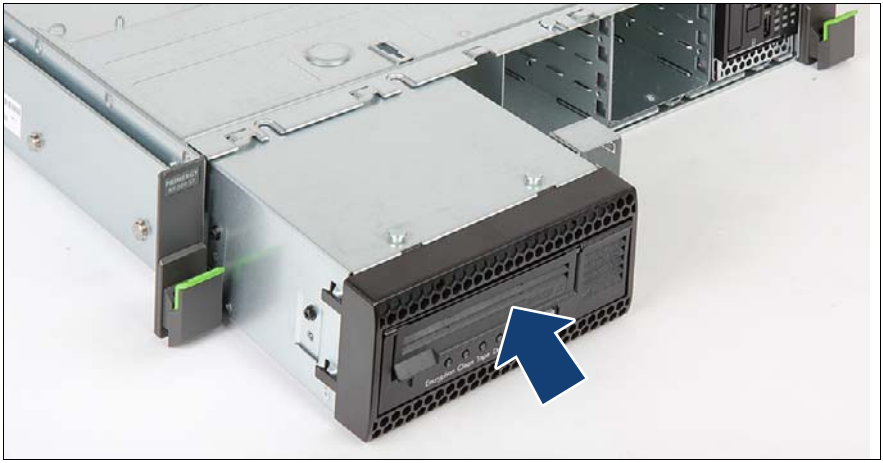


Figure 162: Inserting the LTO cage

- Push the LTO cage into the bay.

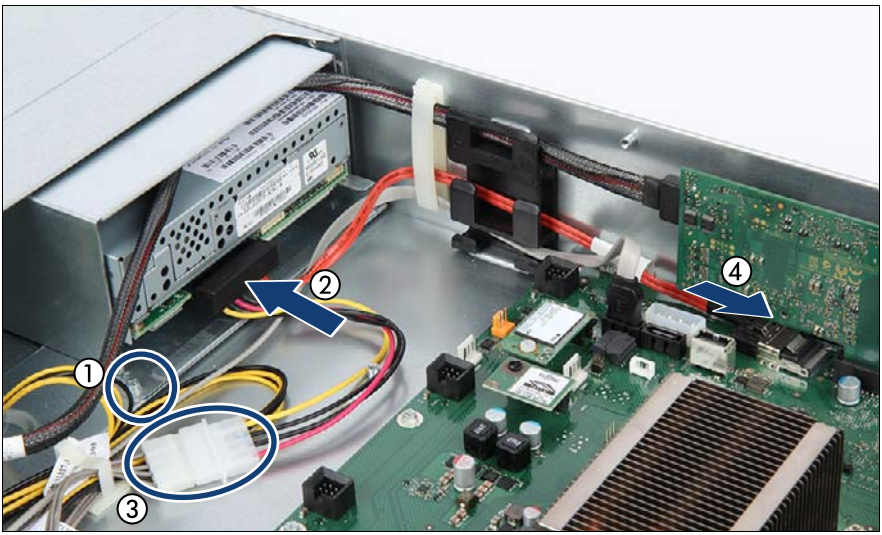


Figure 163: Connecting the cables to the LTO

- Fasten the drive cage with the screw (1).
- Connect the cable to the LTO drive (2).
- Connect the cable to the power cable (3).
- Connect the cable to the system board (4)

12.11.6 Concluding steps

- "Installing the fan box" on page 146
- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- "Verifying and configuring the backup software solution" on page 79
- "Enabling BitLocker functionality" on page 88

12.12 Removing an LTO drive in 2.5-inch version

Upgrade and Repair Unit (URU)

Hardware: 10 minutes

Tools: Phillips PH2 / (+) No. 2 screw driver

12.12.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Locating the defective server" on page 47
- "Removing backup and optical disk media" on page 69
- "Verifying and configuring the backup software solution" on page 69
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51
- "Removing the fan box" on page 144

12.12.2 Removing the drive cage

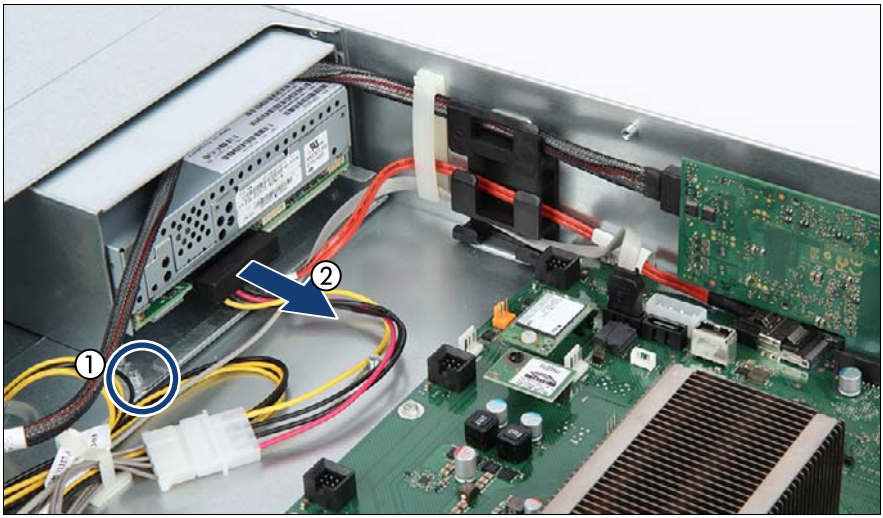


Figure 164: Unlocking the drive cage

- ► Remove the screw that fixed the drive cage in the bay (1).
- ► Remove the cable from the LTO drive (2).

Figure 165: Removing the drive cage

- ► Pull the drive cage out of the bay.

12.12.3 Removing an LTO drive out of the cage

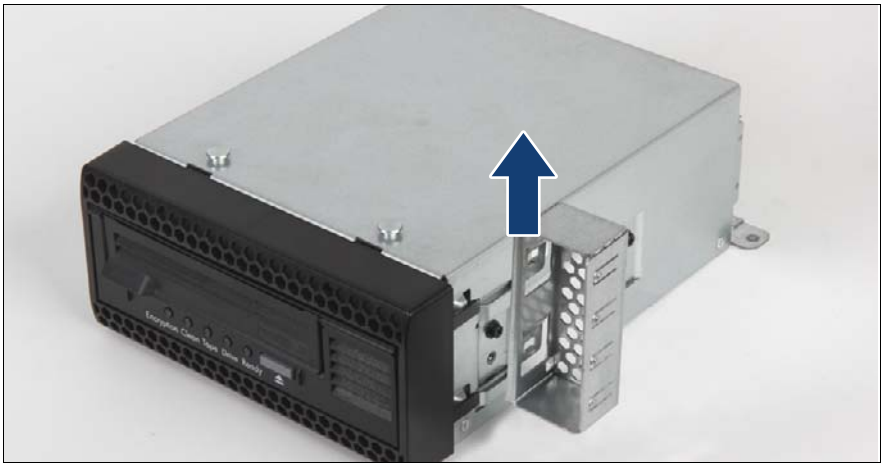


Figure 166: Removing the cover plate

► Remove the cover plate from the drive cage.

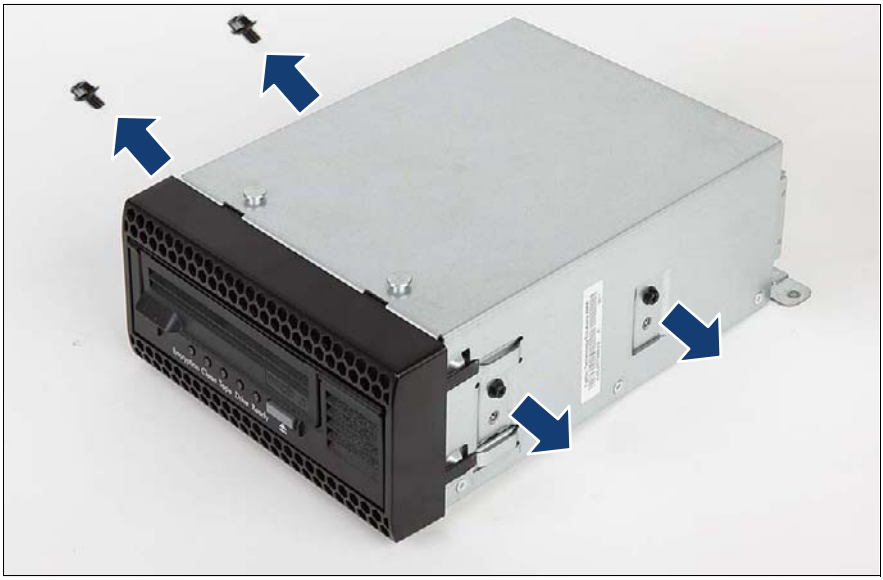


Figure 167: Removing the screws

► Remove the four screws.

Figure 168: Removing the LTO drive

► Pull the LTO drive out.

12.12.4 Installing the tape drive dummy module

Figure 169: Installing the tape drive dummy module (A)

► Push the tape drive dummy module into the drive cage.

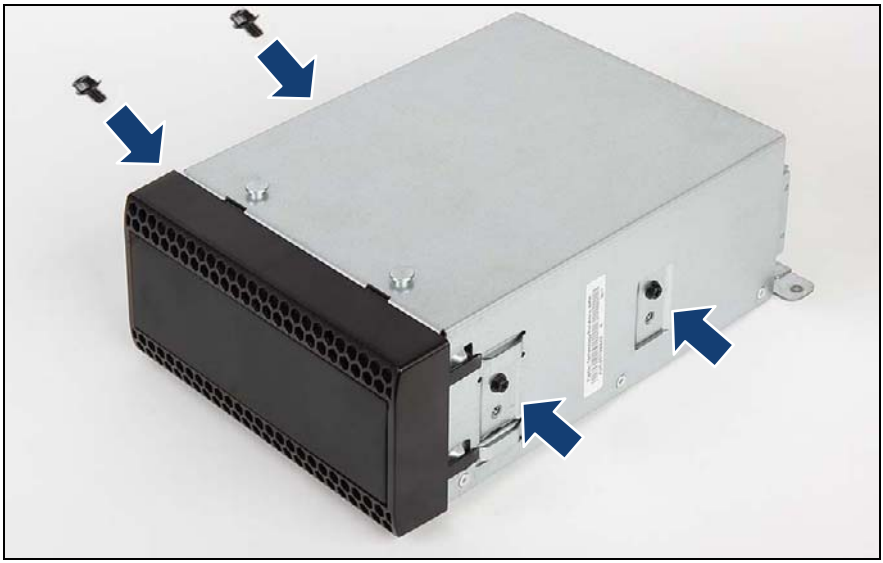


Figure 170: Installing the tape drive dummy module (B)

► Fasten the tape drive dummy module in the drive cage with 4 screws.

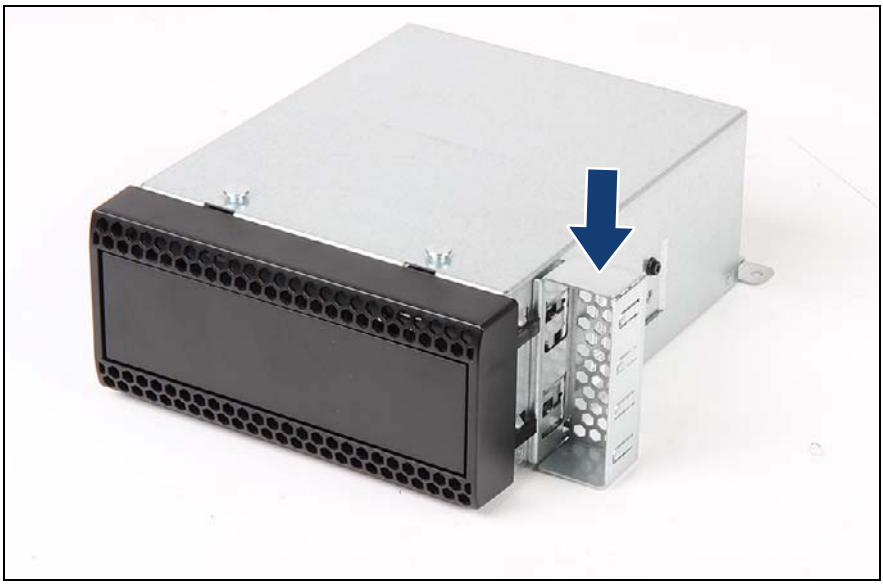


Figure 171: Installing the cover plate

► Fasten the cover plate.

Figure 172: Installing the drive cage with the tape drive dummy module

- Push the drive cage in.
- Fasten the drive cage with the screw see also "Installing the LTO cage" on page 261.

12.12.5 Concluding steps

- "Installing the fan box" on page 146
- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- "Verifying and configuring the backup software solution" on page 79
- "Enabling BitLocker functionality" on page 88

12.13 Replacing the LTO drive in 2.5-inch version

Upgrade and Repair Unit (URU)

Hardware: 10 minutes

Tools: Phillips PH2 / (+) No. 2 screw driver

12.13.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Locating the defective server" on page 47
- "Removing backup and optical disk media" on page 69
- "Verifying and configuring the backup software solution" on page 69
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51
- "Removing the fan box" on page 144

12.13.2 Removing the defective LTO drive

- "Removing the drive cage" on page 264
- "Removing an LTO drive out of the cage" on page 265

12.13.3 Installing the new LTO drive

- "Installing an LTO drive in the cage" on page 259
- "Installing the LTO cage" on page 261

12.13.4 Concluding steps

- "Installing the fan box" on page 146

- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- "Verifying and configuring the backup software solution" on page 79
- "Enabling BitLocker functionality" on page 88

13 Front panel and external connectors

Safety notes

CAUTION!

- When inserting the front panel module into the server, ensure not to pinch or strain any connected cables.
- Circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. Always discharge static build-up (e.g. by touching a grounded object) before handling electrostatic-sensitive devices (ESDs)
- Do not touch the circuitry on boards or soldered parts. Hold circuit boards by their metallic areas or edges.
- For further information, please refer to chapter "Important information" on page 35.

13.1 Front panel module

13.1.1 Replacing the front panel module

Field Replaceable Unit (FRU)

Hardware: 10 minutes
Software: 5 minutes

Tools:	Phillips PH2 / (+) No. 2 screw driver

Note on system information backup / restore

The front panel module contains the Chassis ID EPROM that contains system information like server name and model, housing type, serial number and manufacturing data.

To avoid the loss of non-default settings when replacing the system board, a backup copy of important system configuration data is automatically stored from the system board NVRAM to the Chassis ID EPROM. After replacing the system board the backup data is restored from the Chassis ID board to the new system board.

CAUTION!

For that reason the front panel module and system board must not be replaced simultaneously! In this case, restoring the system configuration data on the system board would fail.

13.1.1.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Disabling SVOM boot watchdog functionality" on page 66
- "Locating the defective server" on page 47
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51
- "Removing the fan box" on page 144

13.1.1.2 Removing the front panel module

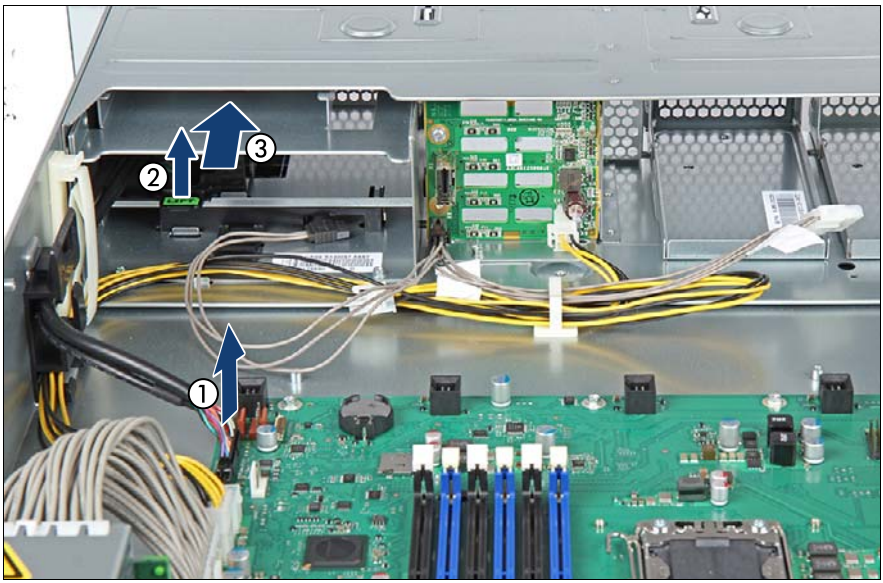


Figure 173: Disconnecting the front panel cable

- ► Disconnect the front panel cable from the system board (1).
- ► If applicable, disconnect the front VGA cable from the system board see section "Removing the front VGA cable" on page 282.
- ► Push the locking latches upward (2) to disengage the locking mechanism.
- ► Carefully pull the front panel module out of its bay (3).

CAUTION!

Ensure that none of the cables are strained or damaged!

- ► If the front VGA connector has been installed in the defective front panel module, remove the cable as described in section "Removing the front VGA connector" on page 283.

13.1.1.3 Installing the front panel module

- ► If the front VGA connection is to be installed in the new front panel module, install the front VGA cable as described in section "Installing the front VGA connector" on page 278.

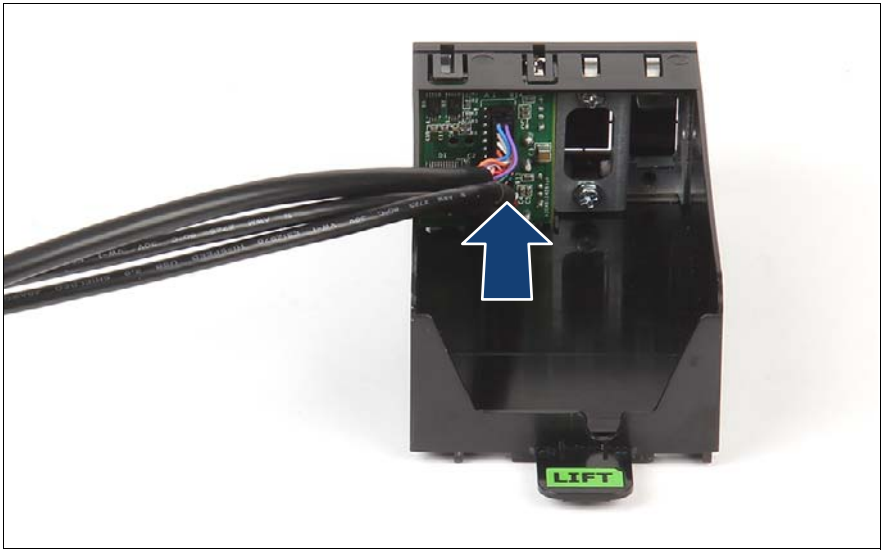


Figure 174: Connecting the front panel cable to the front panel module

► Connect the front panel cable to the new front panel module as shown.

Figure 175: Connecting the front panel cable

► Insert the front panel module into the front panel cage and carefully push in until it locks in place.

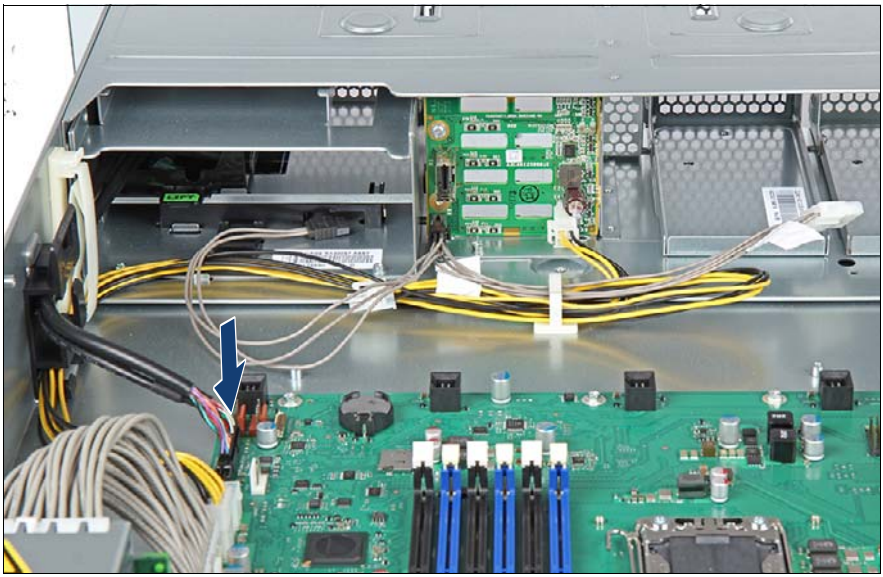


Figure 176: Connecting front panel cables

- Connect the front panel cable to the system board.
- Run the front panel cable through the cable clamps as shown.
- If applicable, connect the front VGA cable to the front VGA connector of the system board as described in section "Installing the front VGA connector" on page 278.

13.1.1.4 Concluding steps

- "Installing the fan box" on page 146
- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- "Verifying system information backup / restore" on page 75
- Store your server's system information on the Chassis ID EPROM integrated into the front panel board. For further information on how to obtain and use the *ChassisId_Prom* Tool, refer to section "Using the Chassis ID Prom Tool" on page 91.

- "Enabling SVOM boot watchdog functionality" on page 82
- "Enabling BitLocker functionality" on page 88

13.2 Front VGA connector

13.2.1 Installing the front VGA connector

Field Replaceable Unit (FRU)

Hardware: 10 minutes

Tools:	Socket screw driver (5 mm) Wrench key for UNC #4-40 hexagon bolts

13.2.1.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Locating the defective server" on page 47
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51
- "Removing the fan box" on page 144

13.2.1.2 Removing the front panel module

- "Removing the front panel module" on page 275

13.2.1.3 Preparing the front panel module

Figure 177: Breaking out the front VGA cover plate

► Break out the VGA cover plate on the front panel cover.

Please note that once removed, the VGA cover plate cannot be refitted.

13.2.1.4 Installing the front VGA connector

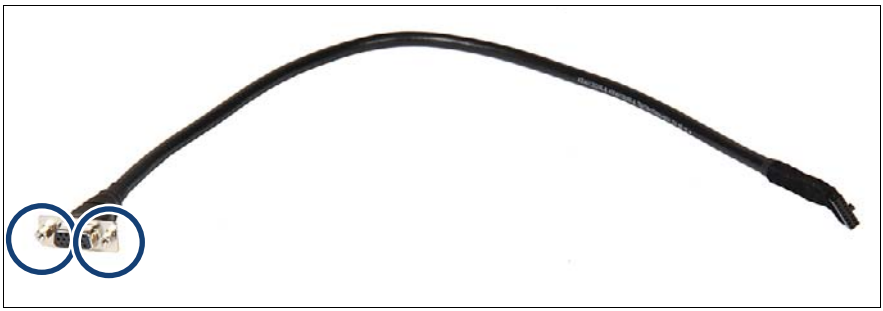


Figure 178: Front VAG cable

► Remove the two hexagon bolts from the connector.

Figure 179: Mounting the front VGA connector

- Insert the front VGA connector with the longer connector side to the left.
- Fasten the front VGA connector in the front panel module with two hexagon bolts.

13.2.1.5 Re-installing the front panel module

- "Installing the front panel module" on page 275

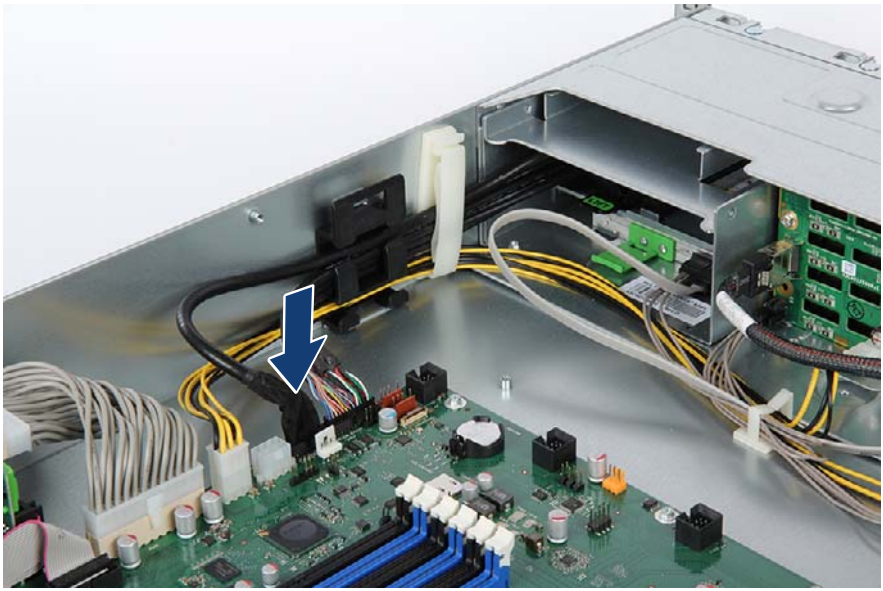


Figure 180: Connecting front panel cables

- Connect the front VGA cable to the system board.
- Run the front VGA cable through the cable clamps as shown.

13.2.1.6 Concluding steps

Perform the following procedures:

- "Installing the fan box" on page 146
- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- "Enabling BitLocker functionality" on page 88

13.2.2 Removing the front VGA connector

Field Replaceable Unit (FRU)

Hardware: 10 minutes

Tools:	Socket screw driver (5 mm) Wrench key for UNC #4-40 hexagon bolts

13.2.2.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Locating the defective server" on page 47
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51
- "Removing the fan box" on page 144

13.2.2.2 Removing the front VGA cable

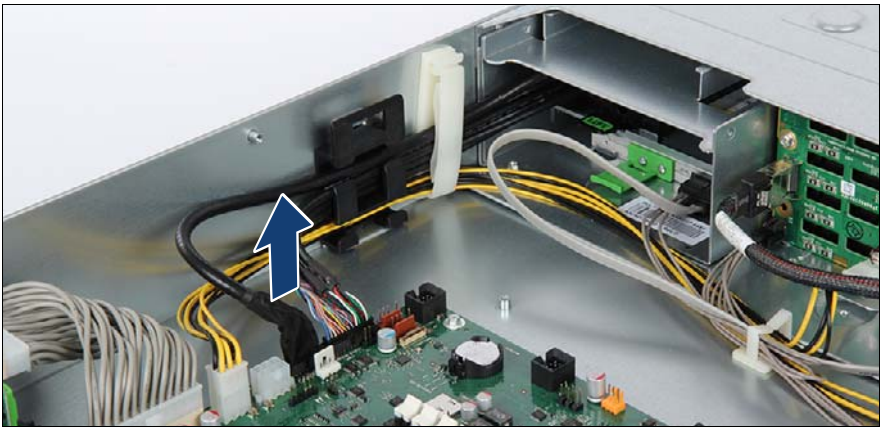


Figure 181: Disconnecting the front VGA cable

- Remove the front VGA cable from the system board.
- "Removing the front panel module" on page 275

13.2.2.3 Removing the front VGA connector

Figure 182: Removing front VGA connector from the front panel module

- Remove two hexagon bolts.
- Push the VGA connector out of the front panel module.

13.2.2.4 Re-installing the front panel module

- "Installing the front panel module" on page 275

13.2.2.5 Concluding steps

- "Installing the fan box" on page 146
- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- "Enabling BitLocker functionality" on page 88

13.2.3 Replacing the front VGA connector

Field Replaceable Unit (FRU)

Hardware: 15 minutes

Tools:	Socket screw driver (5 mm) Wrench key for UNC #4-40 hexagon bolts

13.2.3.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Locating the defective server" on page 47
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51
- "Removing the fan box" on page 144

13.2.3.2 Removing the front panel module

- "Removing the front panel module" on page 278

13.2.3.3 Removing the front VGA connector

- "Removing the front VGA connector" on page 283.

13.2.3.4 Installing the new front VGA connector

- Install the new front VGA connector as described in section "Installing the front VGA connector" on page 279.

13.2.3.5 Re-installing the front panel module

- "Installing the front panel module" on page 275.

13.2.3.6 Concluding steps

- "Installing the fan box" on page 146

- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- "Enabling BitLocker functionality" on page 88

13.3 Front cage

13.3.1 Replacing the front panel cage

Upgrade and Repair Unit (URU)

Hardware: 10 minutes

Tools:	Phillips PH2 / (+) No. 2 screw driver

13.3.1.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Locating the defective server" on page 47
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51
- "Removing the fan box" on page 144

13.3.1.2 Removing the front panel cage

- Disconnect all cables from the modules that are installed in the front panel cage.
  - Front panel cable
  - Front VGA cable
  - ODD cable
  - LSD cable

Multicage

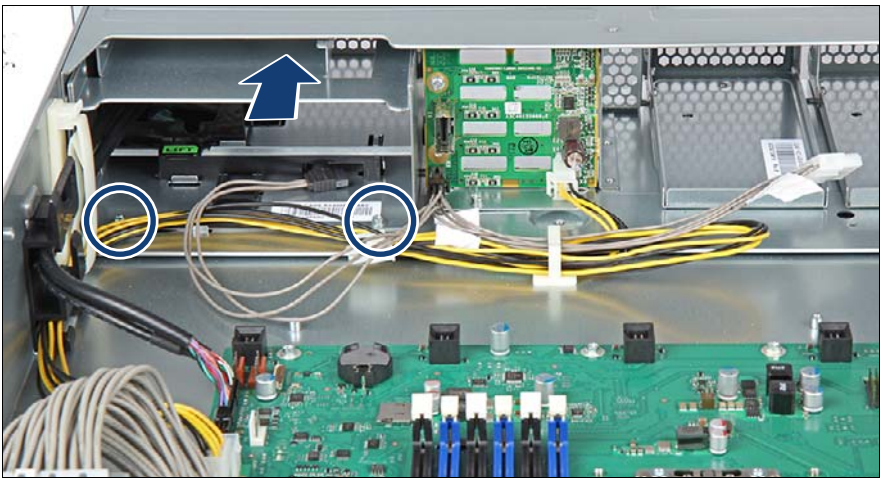


Figure 183: Removing the multicage

- ► Remove the two screws.
- ► Push the multicage out of the chassis frontward.
- ► Remove the installed modules.
  - – "Removing the front panel module" on page 275
  - – "Removing the ODD" on page 242
  - – "Removing the LSD module" on page 233

Panelhousing

Figure 184: Removing the panelhousing

- ► Remove the screw.
- ► Push the panelhousing out of the chassis frontward.
- ► "Removing the front panel module" on page 275

13.3.1.3 Re-installing the front panel cage

Multicage

- ► Install the removed modules.
  - – "Installing the front panel module" on page 275
  - – "Installing an ODD" on page 240
  - – "Installing a LSD module" on page 231

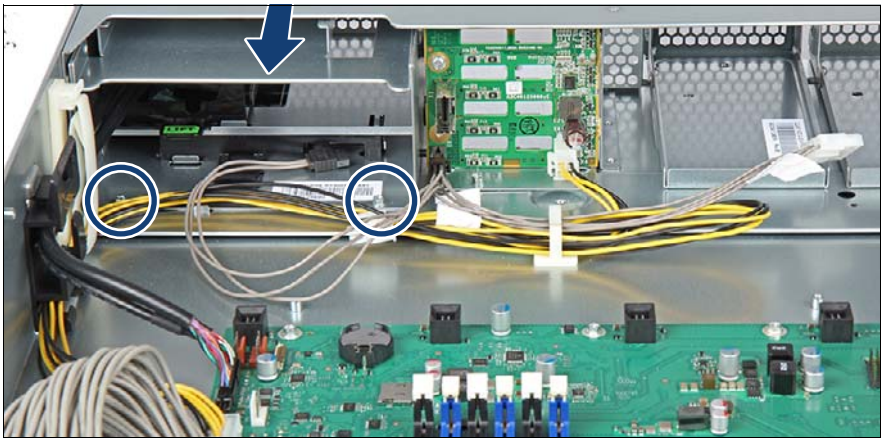


Figure 185: Inserting the front panel cage

- Insert the front panel cage.
- Fasten the front panel cage with two screws

Panelhousing

- "Installing the front panel module" on page 275

Figure 186: Inserting the front panel cage

- Insert the front panel cage.
- Fasten the front panel cage with the screw.

13.3.1.4 Concluding steps

► Connect all cables from the modules that are installed in the front panel cage.

  – Front panel cable:
  – Front VGA cable:
  – ODD cable:
  – LSD cable:

► "Installing the fan box" on page 146

► "Reassembling" on page 57

► "Connecting the server to the power source" on page 62

► "Switching on the server" on page 64

► "Enabling BitLocker functionality" on page 88

14 System board and components

Safety notes

CAUTION!

- Devices and components inside the server remain hot after shutdown. After shutting down the server, wait for hot components to cool down before installing or removing internal options.
- Circuit boards and soldered parts of internal options are exposed and can be damaged by static electricity. Always discharge static build-up (e.g. by touching a grounded object) before handling electrostatic-sensitive devices (ESDs).
- Do not touch the circuitry on boards or soldered parts. Hold circuit boards by their metallic areas or edges.
- For further information, please refer to chapter "Important information" on page 35.

14.1 Basic information

- CMOS battery

  CMOS memory (volatile BIOS memory) and the real-time clock are powered by a lithium coin cell (CMOS battery). This cell lasts up to ten years, depending on ambient temperature and use.

  If the CMOS battery is depleted or falls below minimum voltage levels, it need to be replaced immediately.

- UFM (USB Flash Module)

  The server can be equipped with a USB Flash Module (UFM).

- TPM (Trusted Platform Module)

  The system board is optionally equipped with a Trusted Platform Module (TPM). This module enables programs from third party manufacturers to store key information, for example drive encryption using Windows Bitlocker Drive Encryption.

- Onboard SAS enabling key

The onboard SAS enabling key enables the SAS functionality of the Onboard controller.

14.2 Replacing the CMOS battery

Upgrade and Repair Unit (URU)

Hardware: 5 minutes

Tools: tool-less; recommended: tooth pick

Safety notes

CAUTION!

- The CMOS battery must be replaced with an identical battery or with a battery type recommended by the manufacturer.
- Keep lithium batteries away from children.
- Do not throw batteries into the trash can. Lithium batteries must be disposed of in accordance with local regulations concerning special waste.
- For further safety information, please refer to section "Environmental protection" in the operating manual of your server.
- **Ensure to insert the CMOS battery with the positive pole facing up!**

14.2.1 Preliminary steps

- ► "Locating the defective server" on page 47
- ► "Shutting down the server" on page 49
- ► "Disconnecting power cords" on page 50
- ► "Getting access to the component" on page 51

14.2.2 Removing the battery

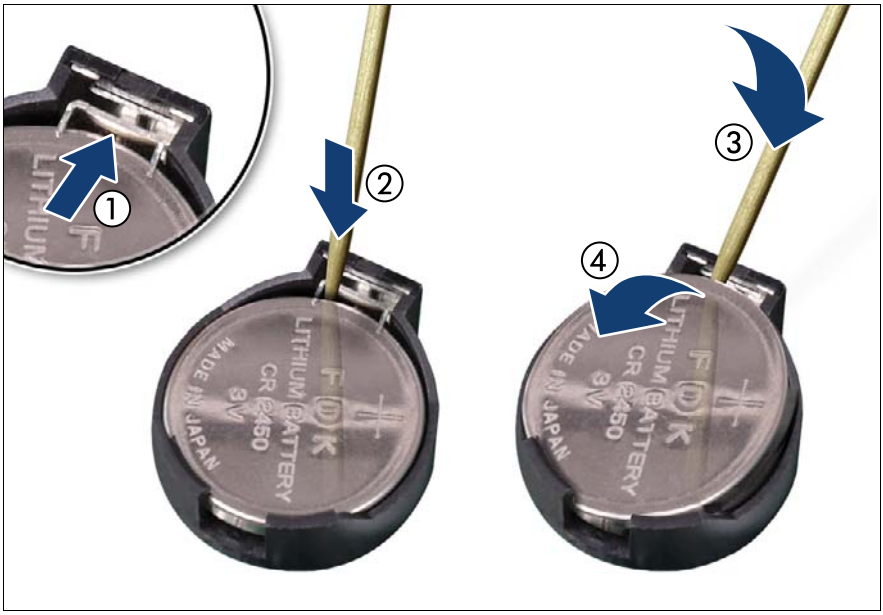


Figure 187: Replacing the CMOS battery

- ► Press out on the locking spring to eject the depleted CMOS battery (1).
- ► If the CMOS battery cannot be ejected this way, use a toothpick (recommended) or similar tool as a lever: Insert the toothpick between the battery and locking spring as shown (2).

CAUTION!

Do not use sharp-edged tools like screw drivers as they may damage system board components when slipping.

- ► Carefully pry the depleted CMOS battery out of its socket as shown (3).
- ► Remove the CMOS battery (4).

Do not throw the CMOS battery into the trash can. Lithium batteries must be disposed of in accordance with local regulations concerning special waste.

14.2.3 Installing the CMOS battery

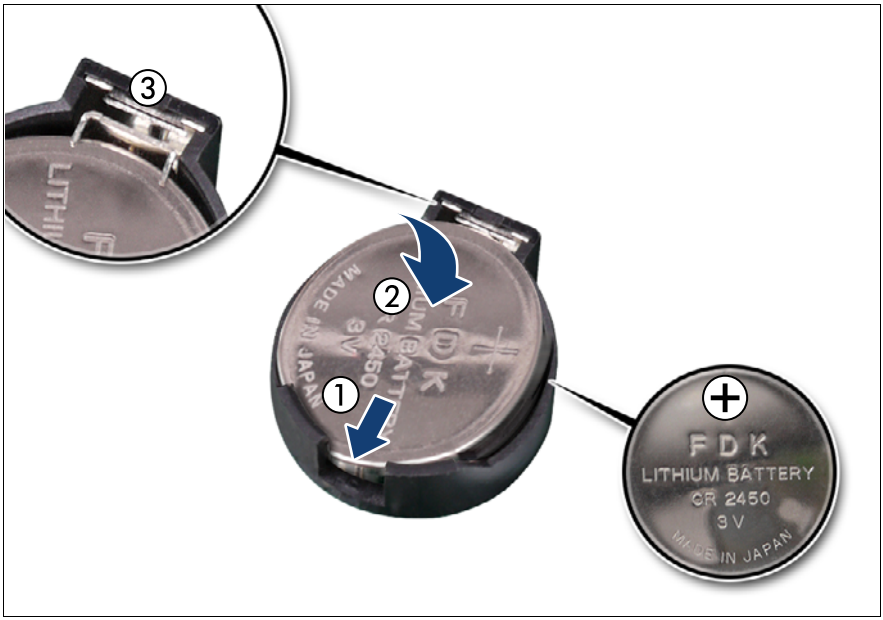


Figure 188: Installing the CMOS battery

- ► At a slight angle, fit the new CMOS battery into its socket as shown (1).

  CAUTION!

  Ensure to insert the CMOS battery with the positive pole (label side) facing up as shown (see close-up).

- ► Fold down the CMOS battery (2) until it locks in place.
- ► Ensure that the locking spring (3) is properly engaged.

14.2.4 Concluding steps

- ► Dispose of the CMOS battery in accordance with local regulations concerning special waste.
- ► "Reassembling" on page 57
- ► "Connecting the server to the power source" on page 62

- "Switching on the server" on page 64
- "Verifying system information backup / restore" on page 75
- "Verifying the system time settings" on page 84

14.3 USB Flash Module (UFM)

This section provides information on how to install, remove or replace the USB Flash Module (UFM).

14.3.1 Installing the UFM

Field Replaceable Unit (FRU)

Hardware: 5 minutes
Software: 5 minutes

Tools: tool-less

14.3.1.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Disabling SVOM boot watchdog functionality" on page 66
- "Locating the defective server" on page 47
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

14.3.1.2 Installing the UFM

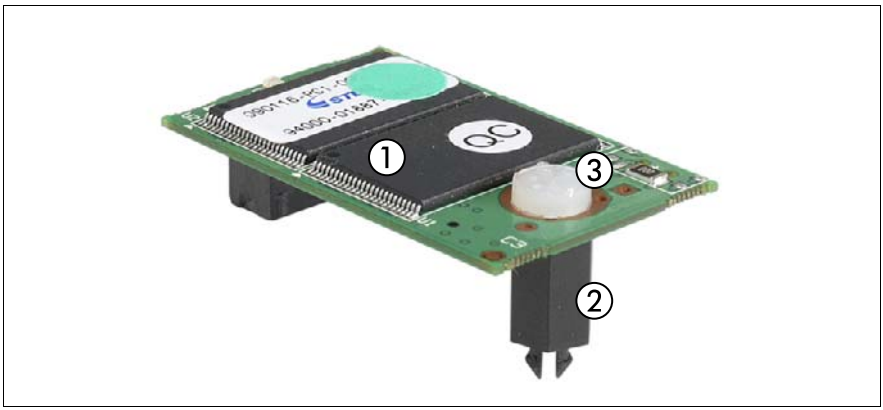


Figure 189: UFM kit

1	USB Flash Module (UFM)	2	UFM spacer
3	UFM nylon screw		

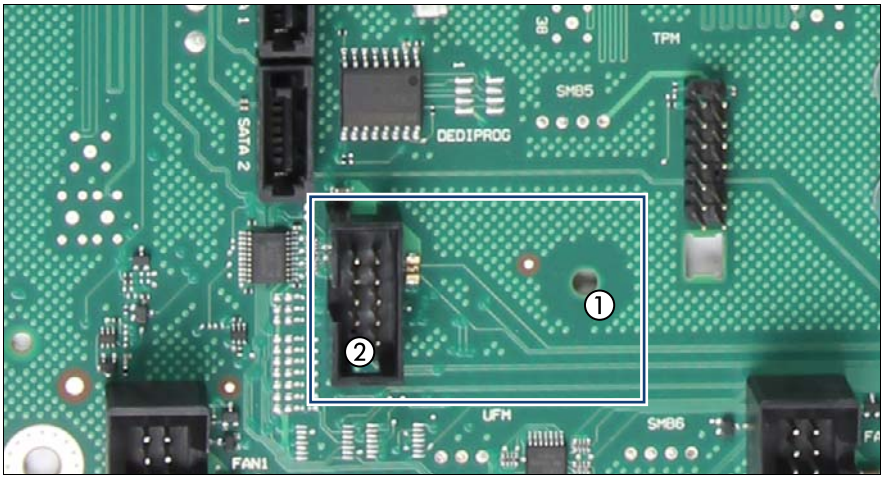


Figure 190: UFM mounting location

1	Cut-out for UFM spacer	2	UFM connector

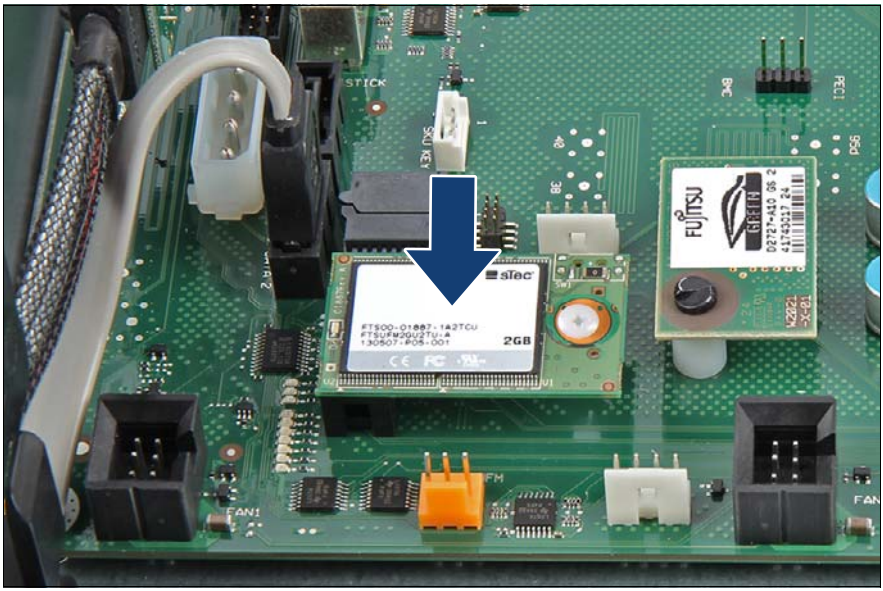


Figure 191: Installing the UFM

► Connect the UFM to the system board, snapping in the UFM spacer.

14.3.1.3 Concluding steps

► "Reassembling" on page 57

► "Connecting the server to the power source" on page 62

► "Switching on the server" on page 64

► "Enabling SVOM boot watchdog functionality" on page 82

► "Enabling BitLocker functionality" on page 88

14.3.1.4 Software configuration

The UFM delivery set includes the "Recovery Tool CD" to setup the ESXi configuration. Proceed as follows:

► Switch on the server.

► Right after switching on the server, insert the "Recovery Tool CD" into the DVD drive and close the drive tray.

- The server should now boot from the "Recovery Tool CD".
- Follow the on-screen instructions.

14.3.2 Removing the UFM

Field Replaceable Unit (FRU)

Hardware: 5 minutes

Tools:	Phillips PH0 / (+) No. 0 screw driver

14.3.2.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Locating the defective server" on page 47
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

14.3.2.2 Removing the UFM

Figure 192: Removing the UFM (A)

- ► Remove the nylon screw on the defective UFM (1).
- ► Disconnect and remove the defective UFM (2).
- ► The UFM spacer remains on the system board.

14.3.2.3 Concluding steps

- ► "Reassembling" on page 57
- ► "Connecting the server to the power source" on page 62
- ► "Switching on the server" on page 64
- ► "Enabling BitLocker functionality" on page 88

14.3.3 Replacing the UFM

Upgrade and Repair Unit (URU)

Hardware: 10 minutes
Software: 5 minutes

Tools:	– Phillips PH0 / (+) No. 0 screw driver – combination pliers and flat nose pliers

14.3.3.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Disabling SVOM boot watchdog functionality" on page 66
- "Locating the defective server" on page 47
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

14.3.3.2 Removing the UFM

- "Removing the UFM" on page 298
- The UFM spacer remains on the system board.

14.3.3.3 Installing the new UFM

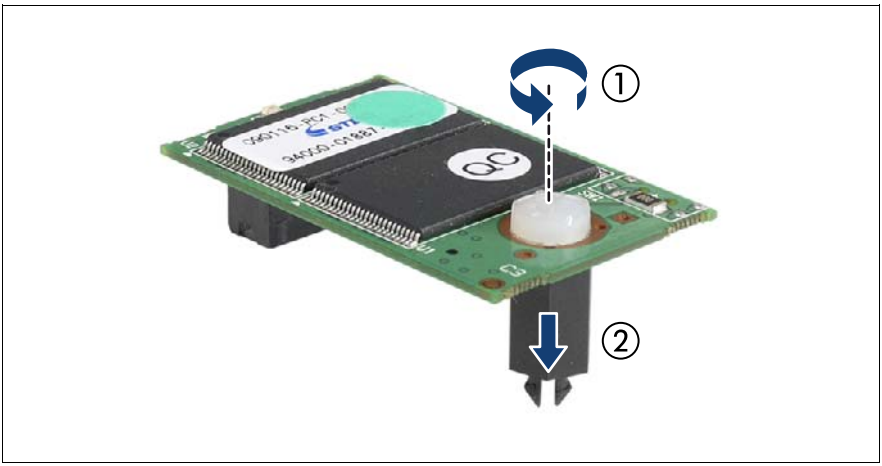


Figure 193: Preparing the new UFM

- Remove the nylon screw from the new UFM (1).

► Remove the UFM spacer (2).

Figure 194: Installing the UFM (B)

► Fit the new UFM on the UFM connector and the remaining UFM spacer (1).

► Secure the UFM to the UFM spacer with the nylon screw (2).

Destroying the defective UFM

CAUTION!

The UFM contains customer information (e.g. IP address, license numbers). After replacing the UFM, hand the defective UFM over to the customer. If the customer requests disposal of the defective UFM, proceed as follows:

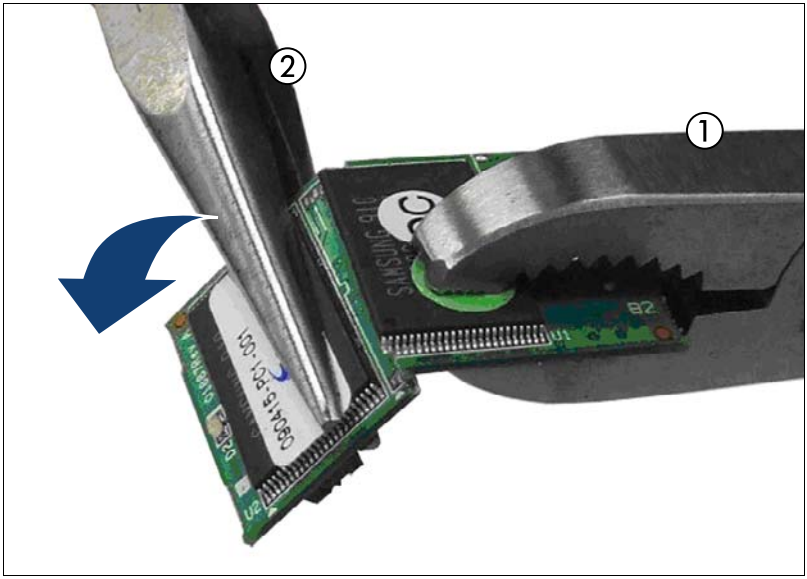


Figure 195: Destroying the defective UFM

► Use a pair of combination pliers (1) and flat nose pliers (2) to break the UFM in half as shown.

14.3.3.4 Concluding steps

- "Installing the air duct" on page 57
- "Mounting the housing cover" on page 59
- "Sliding the server into the rack" on page 62

  If the server has been completely removed from the rack for maintenance purposes, reinstall and secure it in the rack as described in section "Mounting the server in the rack" on page 59.
- "Connecting the server to the power source" on page 62
- "Enabling SVOM boot watchdog functionality" on page 82
- "Enabling BitLocker functionality" on page 88

14.3.3.5 Software configuration

The UFM delivery set includes the "Recovery Tool CD" to setup the ESXi configuration. Proceed as follows:

- Switch on the server.
- Right after switching on the server, insert the "Recovery Tool CD" into the DVD drive and close the drive tray.
- The server should now boot from the "Recovery Tool CD".
- Follow the on-screen instructions.

14.4 Trusted Platform Module (TPM)

14.4.1 Installing the TPM

Upgrade and Repair Unit (URU)

Hardware: 5 minutes
Software: 5 minutes

Tools: Phillips PH2 / (+) No. 2 screw driver

Installing the TPM:

– Bit screw driver
– TPM bit insert (*)

(*) For the Japanese market:

– TPM module fixing tool (S26361-F3552-L909)

14.4.1.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Locating the defective server" on page 47
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

14.4.1.2 Installing the TPM

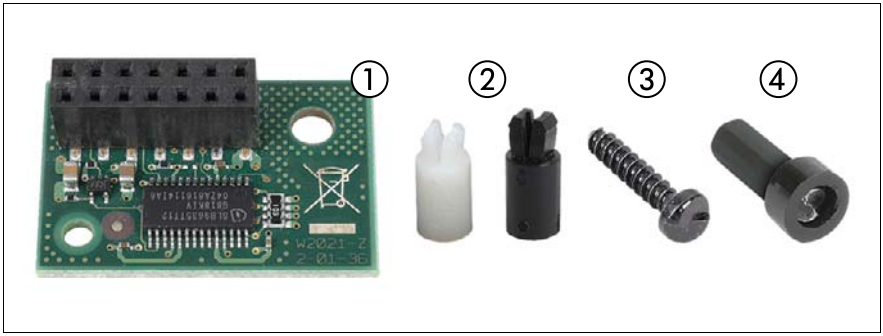


Figure 196: TPM kit

1	TPM (Trusted Platform Module)	3	Special screw for TPM
2	TPM spacer The black TPM spacer is not used in this server.	4	TPM bit insert for TPM special screw

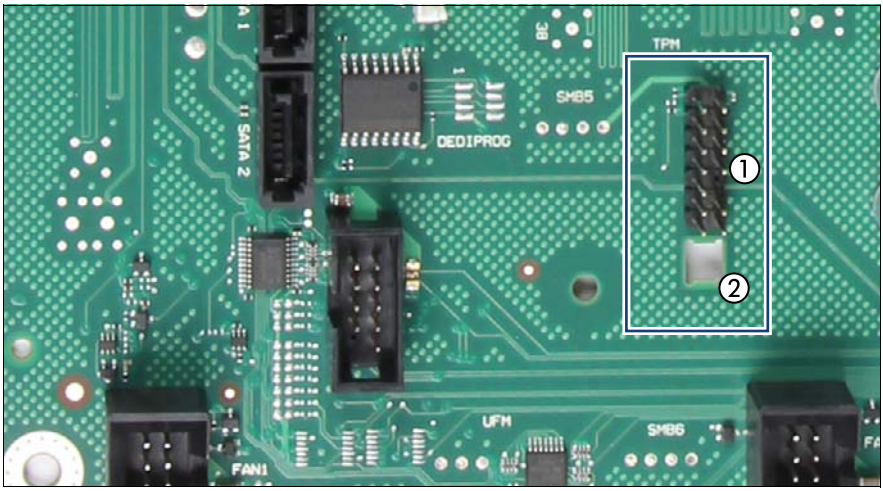


Figure 197: TPM mounting location

1	TPM connector	2	Cut-out for TPM spacer

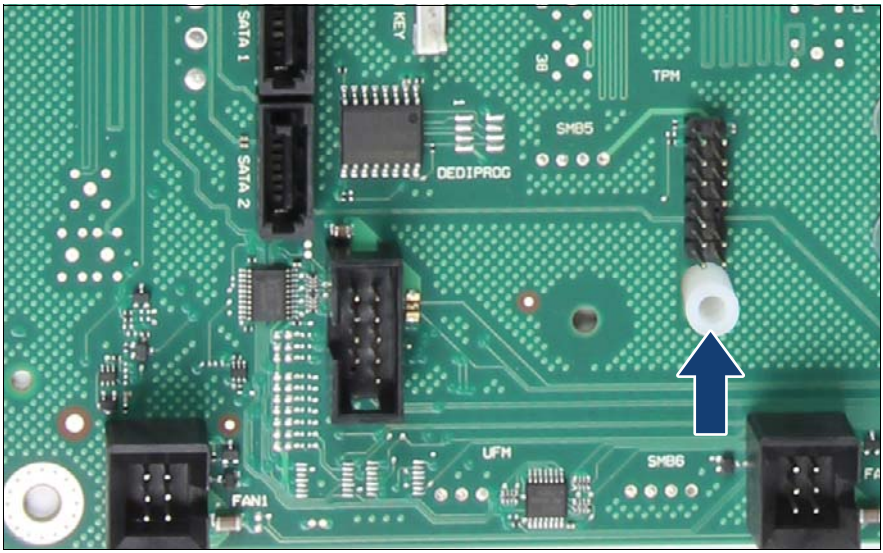


Figure 198: Installing the TPM spacer

► Snap the TPM spacer into the cut-out in the system board.

Figure 199: TPM bit insert

► Attach the TPM bit insert or TPM module fixing tool (Japanese market) to a bit screw driver.

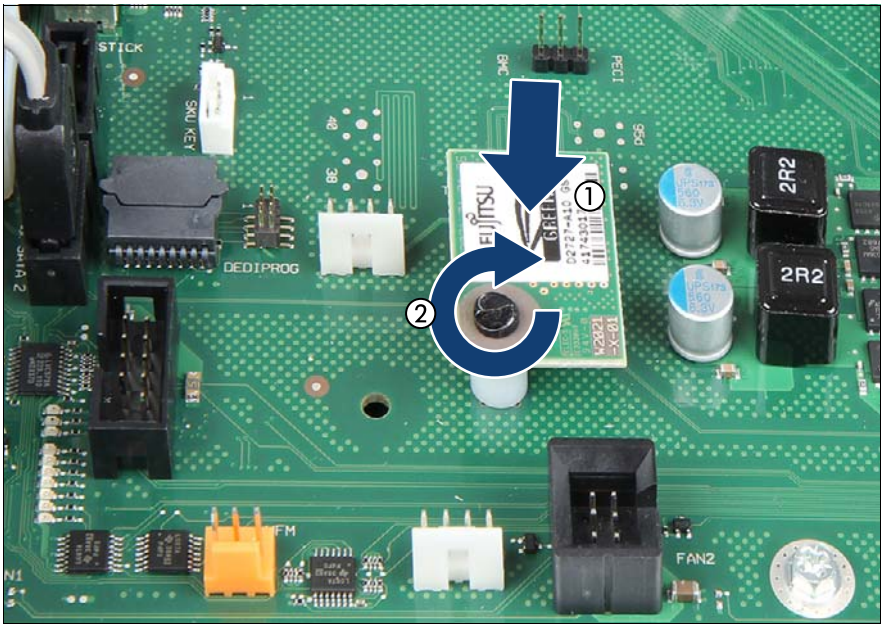


Figure 200: Securing the TPM

- Connect the new TPM to the system board.
- Secure the TPM with the TPM screw using the TPM bit insert.

  Do not fasten the screw too firmly. Stop as soon as the head of the screw lightly touches the TPM.

14.4.1.3 Concluding steps

- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- Enable TPM in the system board BIOS. Proceed as follows:
  - Switch on or restart your server.
  - As soon as the startup screen appears, press the F2 function key to enter the BIOS.
  - Select the *Advanced* menu.
  - Select the *Trusted Computing* submenu.

- ► Set the *TPM Support* and *TPM State* settings to *Enabled*.
- ► Under *Pending TPM operation*, select the desired TPM operation mode.
- ► Save your changes and exit the BIOS.

For detailed information on how to access the BIOS and modify settings, refer to the corresponding BIOS Setup Utilty reference manual available online at *http://jp.fujitsu.com/platform/server/primergy/manual/*.

► "Switching on the server" on page 64

► "Enabling BitLocker functionality" on page 88

14.4.2 Removing the TPM

Field Replaceable Unit (FRU)

Hardware: 30 minutes

Tools: Removing the system board:

– Phillips PH2 / (+) No. 2 screw driver

Removing the TPM:

– flat nose pliers
– thin slotted screw driver (2 x 0.4 mm) (*)

(*) For the Japanese market:

– Dedicated TPM screw driver (CWZ8291A)

CAUTION!

Advise your contact persons that they must provide you with TPM backup copies. For security reasons, the TPM must be restored/re-saved by the customer. After installing a new system board, the TPM must be enabled. You may not clear the TPM data.

If the contact persons **DO NOT** have a backup copy available, inform them that replacing the TPM will cause to lose all data.

14.4.2.1 Preliminary steps

► Before removing the TPM, it is necessary to remove BitLocker-protection from the computer and to decrypt the volume.

Ask the system administrator to turn off BitLocker-protection using the BitLocker setup wizard available either from the Control Panel or Windows Explorer:

► Open Bitlocker Drive Encryption by clicking the *Start* button, clicking *Control Panel*, clicking *Security*, and then clicking *Bitlocker Drive Encryption*.

Administrator permission required. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.

► To turn off BitLocker and decrypt the volume, click *Turn Off BitLocker*, and then click *Decrypt the volume*.

Decrypting the volume may be time-consuming. By decrypting the volume, all of the information stored on that computer is decrypted.

For further information on how to disable BitLocker drive encryption, please refer to the Microsoft Knowledge Base.

Fujitsu service partners will find additional information (also available in Japanese) on the Fujitsu Extranet web pages.

► Disable TPM in the system board BIOS. Proceed as follows:

► Switch on or restart your server.

► As soon as the startup screen appears, press the F2 function key to enter the BIOS.

► Select the *Advanced* menu.

► Select the *Trusted Computing* submenu.

► Set the *TPM Support* and *TPM State* settings to *Disabled*.

► Save your changes and exit the BIOS.

For detailed information on how to access the BIOS and modify settings, refer to the corresponding BIOS Setup Utilty reference manual available online at (*http://jp.fujitsu.com/platform/server/primergy/manual/*.

► "Locating the defective server" on page 47

► "Shutting down the server" on page 49

► "Disconnecting power cords" on page 50

► "Getting access to the component" on page 51

► "Removing the fan box" on page 144

14.4.2.2 Removing the TPM

► "Removing the defective system board" on page 323.

► Lay the system board on a soft, antistatic surface with its component side facing down.

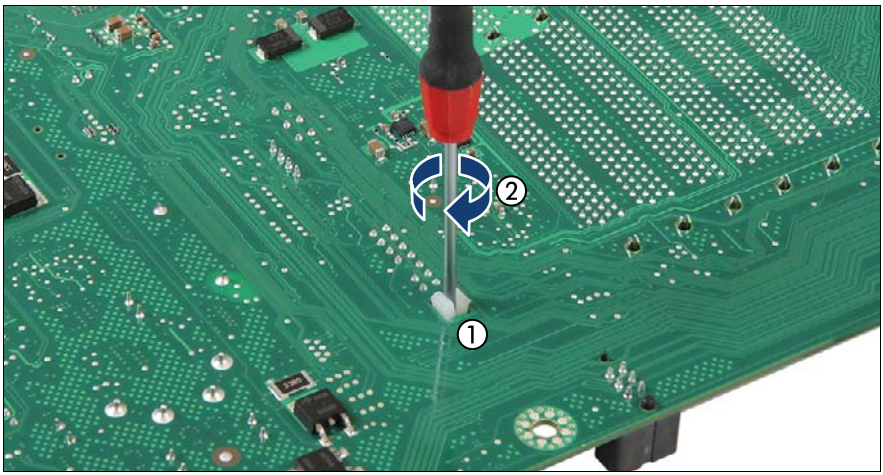


Figure 201: Removing the TPM screw

► Locate the slotted lower end of the TPM screw (1).

- Carefully loosen the TPM screw using a thin slotted screw driver (e.g. watchmaker's screw driver) or the dedicated TPM screw driver (Japanese market) (2).

  CAUTION!

  Ensure to turn the screw **clockwise** in order to remove it!

  Slowly and carefully increase the pressure on the screw until it begins to turn. The effort when loosing the screw should be as low as possible.

  Otherwise the thin metal bar may break, rendering it impossible to loosen the screw.

- Remove the TPM screw.
- Remove the defective TPM on the upper side of the system board.

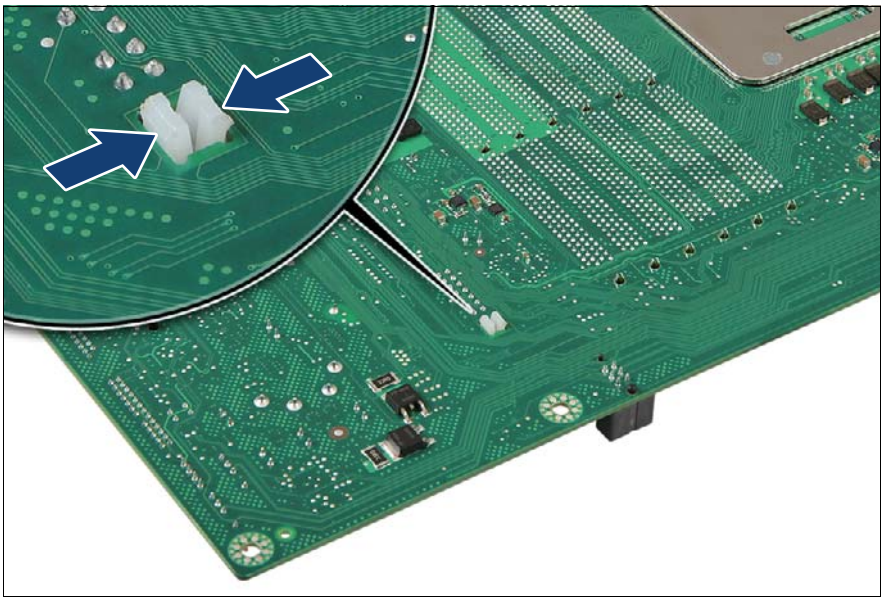


Figure 202: Removing the TPM spacer

- Using a flat nose pliers, press together the hooks on the TPM spacer (see close-up) and remove it from the system board.

  If the TPM is to be replaced, the TPM spacer may remain on the system board.

14.4.2.3 Concluding steps

- "Installing the fan box" on page 146
- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64

14.4.3 Replacing the TPM

Field Replaceable Unit (FRU)

Hardware: 40 minutes

Tools: Removing the system board:

– Phillips PH2 / (+) No. 2 screw driver

Replacing the TPM:

– Bit screw driver
– TPM bit insert (*)
– flat nose pliers
– thin slotted screw driver (2 x 0.4 mm) (*)

(*) For the Japanese market:

– Dedicated TPM screw driver (CWZ8291A)
– TPM module fixing tool (S26361-F3552-L909)

CAUTION!

Advise your contact persons that they must provide you with TPM backup copies. For security reasons, the TPM must be restored/re-saved by the customer. After installing a new system board, the TPM must be enabled. You may not clear the TPM data.

If the contact persons **DO NOT** have a backup copy available, inform them that replacing the TPM will cause to lose all data.

14.4.3.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65

- "Locating the defective server" on page 47
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51
- "Removing the fan box" on page 144

14.4.3.2 Removing the TPM

- "Removing the TPM" on page 309
- Leave the TPM spacer on the system board when removing the defective TPM.

14.4.3.3 Re-installing the TPM

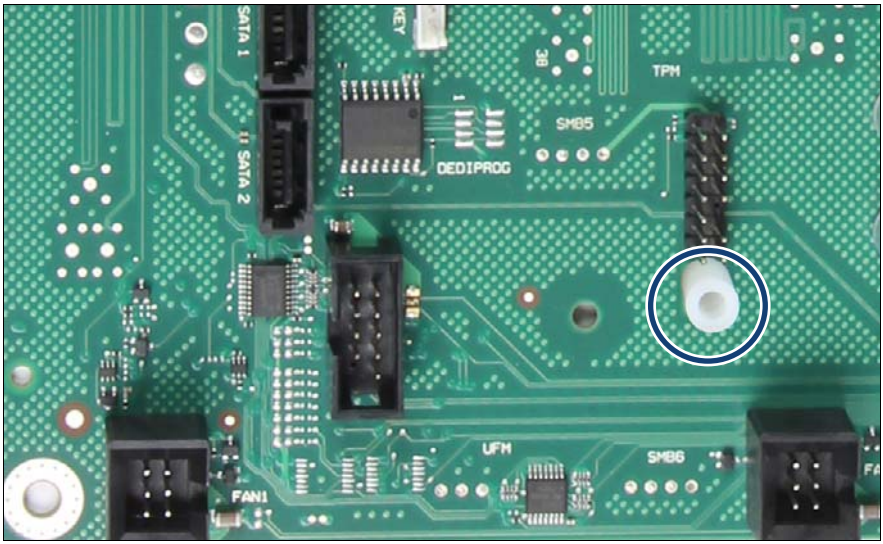


Figure 203: TPM spacer

- The TPM spacer is already present on the system board.
- "Installing the TPM" on page 304

14.4.3.4 Concluding steps

- "Installing the fan box" on page 146
- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- "Enabling BitLocker functionality" on page 88

14.5 Onboard SAS enabling key

The onboard SAS enabling key needs to be installed in order to enable SAS connector SAS 1-4 on the system board.

14.5.1 Installing the onboard SAS enabling key

Field Replaceable Unit (FRU)

Hardware: 5 minutes

Tools: tool-less

14.5.1.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Locating the defective server" on page 47
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

14.5.1.2 Installing the onboard SAS enabling key

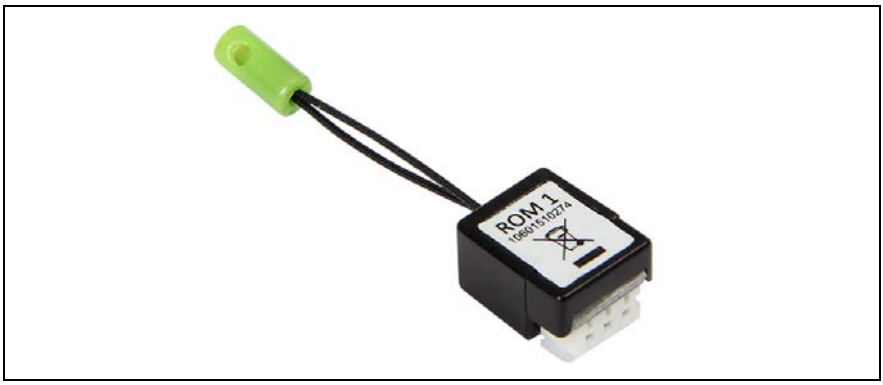


Figure 204: onboard SAS enabling key

► Locate the onboard SAS enabling key mounting location on the system board.

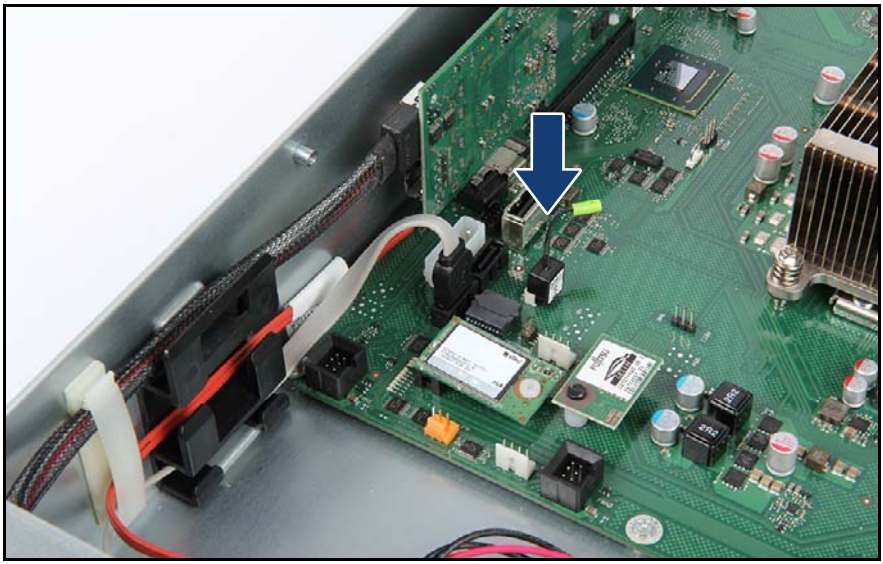


Figure 205: Onboard SAS enabling key mounting location

► Connect the onboard SAS enabling key to system board connector "SKU key".

14.5.1.3 Concluding steps

- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- "Enabling BitLocker functionality" on page 88.

14.5.2 Removing the onboard SAS enabling key

Field Replaceable Unit (FRU)

Hardware: 5 minutes

Tools: tool-less

14.5.2.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Locating the defective server" on page 47
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

14.5.2.2 Removing onboard SAS enabling key

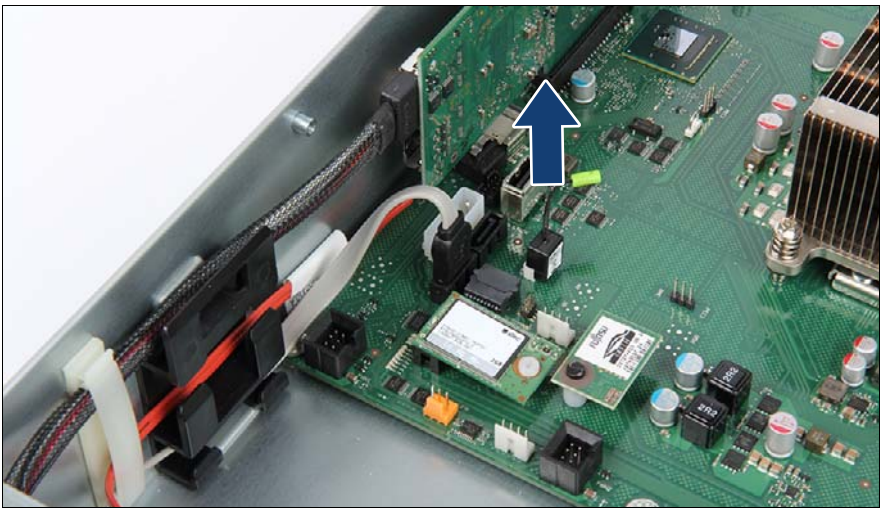


Figure 206: onboard SAS enabling key mounting location

- Firmly pull up on the release lash until the onboard SAS enabling key pops out of its connector.

14.5.2.3 Concluding steps

- "Reassembling" on page 57
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- "Enabling BitLocker functionality" on page 88.

14.5.3 Replacing the onboard SAS enabling key

Field Replaceable Unit (FRU)

Hardware: 5 minutes

Tools: tool-less

14.5.3.1 Preliminary steps

- "Disabling BitLocker functionality" on page 65
- "Locating the defective server" on page 47.
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- "Getting access to the component" on page 51

14.5.3.2 Replacing the onboard SAS enabling key

- "Removing onboard SAS enabling key" on page 318
- "Installing the onboard SAS enabling key" on page 316

14.5.3.3 Concluding steps

- "Reassembling" on page 57.
- "Connecting the server to the power source" on page 62
- "Switching on the server" on page 64
- "Enabling BitLocker functionality" on page 88

14.6 Replacing the system board

Field Replaceable Unit (FRU)

Hardware: 50 minutes
Software: 10 minutes

Tools: Replacing the system board:

– Phillips PH2 / (+) No. 2 screw driver

– Magnifying glass for inspecting processor socket springs (recommended)

Replacing the TPM:

– Bit screw driver
– TPM bit insert (*)
– thin slotted screw driver (2 x 0.4 mm) (*)

(*) For the Japanese market:

– Dedicated TPM screw driver (CWZ8291A)
– TPM module fixing tool (S26361-F3552-L909)

If a UFM is installed:

– Phillips PH1 / (+) No. 1 screw driver

Note on TPM

The system board can be equipped with an optional TPM (Trusted Platform Module). This module enables third party programs to store key information (e. g. drive encryption using Windows Bitlocker Drive Encryption).

If the customer is using TPM functionality, the TPM has to be removed from the defective system board and connected to the new system board. For a detailed description, please refer to section "Replacing the TPM" on page 313.

The TPM is activated in the system BIOS.

CAUTION!

– Before replacing the system board, ask the customer whether TPM functionality is used.

– If the customer is using TPM functionality, remove the TPM from the old system board and install it on the new system board.

  Advise your contact persons that they must provide you with TPM backup copies. For security reasons, the TPM must be restored / re-saved by the customer. After installing a new system board the TPM must be enabled. You may not clear the TPM data.

If the contact persons **DO NOT** have a backup copy available, inform them that replacing the TPM will cause to lose all data.

Note on system information backup / restore

The front panel module contains the Chassis ID EPROM that contains system information like server name and model, housing type, serial number and manufacturing data.

To avoid the loss of non-default settings when replacing the system board, a backup copy of important system configuration data is automatically stored from the system board NVRAM to the Chassis ID EPROM. After replacing the system board the backup data is restored from the Chassis ID board to the new system board.

CAUTION!

For that reason the front panel module and system board must not be replaced simultaneously! In this case, restoring the system configuration data on the system board would fail.

Note on network settings recovery

When replacing network controllers or the system board, network configuration settings in the operating system will be lost and replaced by default values. This applies to all static IP address and LAN teaming configurations.

Ensure to note down your current network settings before replacing a controller or the system board.

14.6.1 Preliminary steps

- "Note on network settings recovery" on page 321
- "Disabling BitLocker functionality" on page 65
- "Disabling SVOM boot watchdog functionality" on page 66
- "Locating the defective server" on page 47
- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- Disconnect all external cables.
- "Getting access to the component" on page 51
- "Removing the fan box" on page 144
- "Removing the power backplane" on page 108

14.6.2 Removing the defective system board

- ► Remove all cables from the system board.
- ► Remove the following components from the system board as shown in the related sections:
  - – Heat sink: see section "Removing processor heat sinks" on page 222

    Leave the processor on the defective board for now.
  - – Memory modules: see section "Removing memory modules" on page 201

    Ensure to take note of the memory modules' mounting positions for reassembly.
  - – Expansion cards: see section "Removing expansion cards" on page 162

    Ensure to take note of the controllers' mounting positions and cable connections for reassembly.
  - – UFM: see section "Removing the UFM" on page 298
  - – onboard SAS enabling key: see section "Removing the onboard SAS enabling key" on page 317
  - – SAS RAID controller: see section "Removing the SAS RAID controller" on page 170

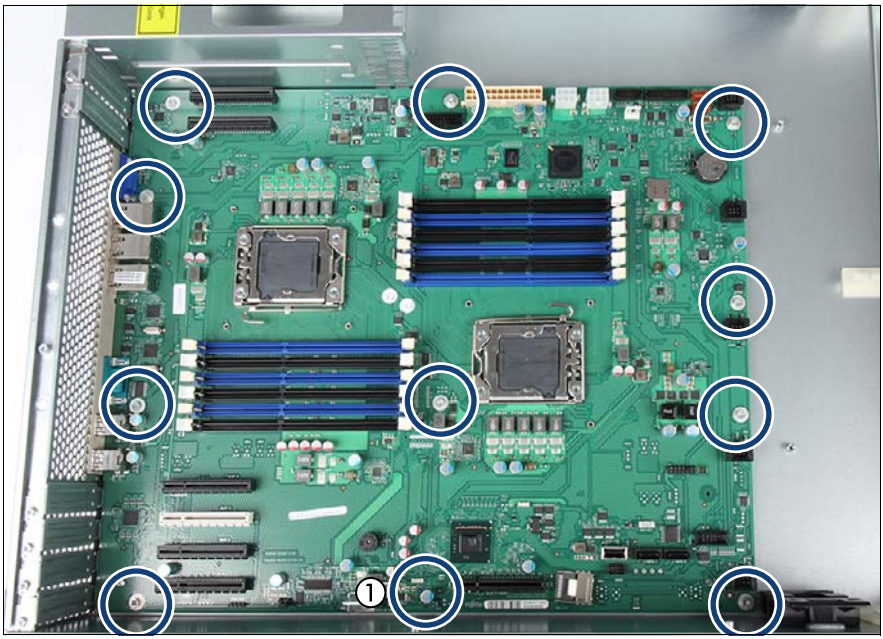


Figure 207: Detaching the system board

► Remove 11 screws from the system board (see circles).

If there was an SAS RAID controller installed the screw (1) is already removed.

Figure 208: Removing the system board

- Slightly lift up the system board by the memory module ejectors and a PCI slot in order to detach it from the centering bolts (C).
- Carefully shift the system board towards the server front until the plug shells disengage from the cut-outs in the connector panel (1).
- Hold the defective system board by the memory module ejectors and a PCI slot and at a slight angle lift it out of the chassis.
- "Removing the TPM" on page 311
- Remove the UFM spacer from the systemboard

14.6.3 Installing the system board

14.6.3.1 Mounting the system board

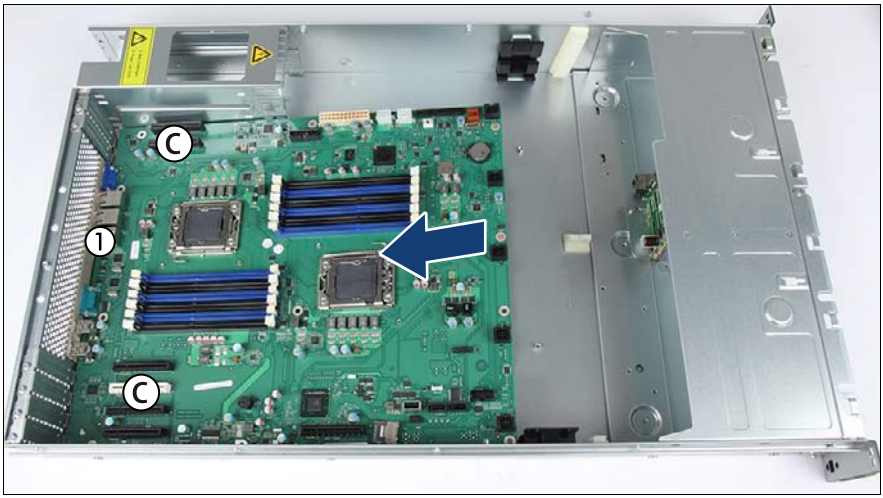


Figure 209: Installing the system board

► Hold the new system board by the memory module ejectors and a PCI slot.

CAUTION!

– Do not lift or handle the system board by any of its heat sinks!

– Ensure not to damage the EMI springs to comply with applicable EMC regulations and satisfy cooling requirements and fire protection measures.

► At a slight angle, lower the system board into the chassis.

► Carefully shift the system board towards the server rear until the plug shells engage with the cut-outs in the connector panel (1).

► Lower the system board onto the centering bolts (C).
Ensure that the system board is properly seated on both centering bolts.

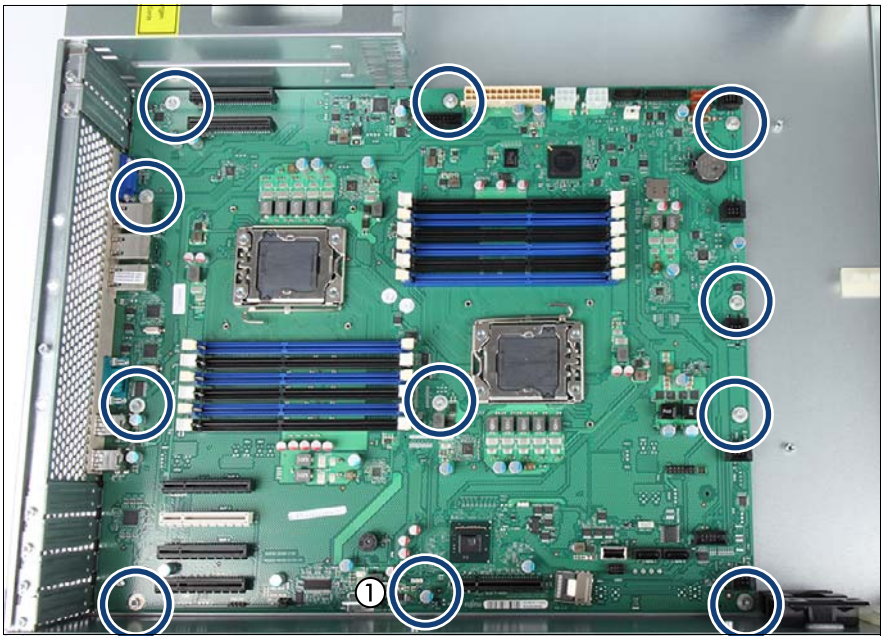


Figure 210: Securing the system board

► Secure the system board with 11 screws (M3 x 6 mm, C26192-Y10-C68) (see circles).

If you want to install a SAS RAID controller, do not insert the screw markt with (1).

Screw torque: 0.6 Nm (not applicable for the Japanese market) Tighten the screws in a cross diagonal pattern.

► Verify the settings on the new system board (see figure "Onboard settings" on page 358).

14.6.3.2 Swapping processors

Preparing the processor socket load plates on the new system board

► "Removing the protective cover" on page 208

Removing processors from the defective system board

- Carefully remove the processors from their sockets on the defective system board as described in "Removing a processor" on page 212.

  Remove and reinstall one processor at a time. Do not remove the second processor from the defective system board until the first processor has been installed on the new system board.

Installing processors on the new system board

- "Installing the processor" on page 207.

Installing protective socket covers on the defective system board

Since the defective system board is sent back for repair, protect the delicate processor socket springs with a socket cover.

- "Removing the protective cover" on page 208

14.6.4 Concluding steps

- Reconnect all cables to the system board. For a complete cabling overview, please refer to section "List of used cables" on page 331.
- Reinstall all remaining system board components as shown in the related sections:
  - SAS RAID controller: see section "Installing the SAS RAID controller" on page 167
  - onboard SAS enabling key: see section "Installing the onboard SAS enabling key" on page 315
  - Heat sinks: see section "Installing processor heat sinks" on page 219
  - Memory modules: see section "Installing a memory module" on page 199

    Install all memory modules into their original slots.
  - Expansion cards: see section "Installing expansion cards" on page 159

    Install all expansion cards into their original slots.

  - UFM: install the UFM spacer to the system board and install the UFM see section "Installing the UFM" on page 295
  - TPM (if applicable): see section "Installing the TPM" on page 304

- "Installing the power backplane" on page 110
- "Installing the fan box" on page 146
- "Reassembling" on page 57
- If applicable, activate TPM functionality in the system BIOS under *Security* > *TPM (Security Chip) Setting* > *Security Chip*. For more information, refer to the corresponding BIOS Setup Utility Reference Manual.
- Reconnect all external cables.
- "Connecting the server to the power source" on page 62
- "Updating or recovering the system board BIOS and iRMC" on page 73
- "Verifying system information backup / restore" on page 75
- "Verifying the system time settings" on page 84
- Inform the customer about changed WWN and MAC addresses. For further information, refer to section "Looking up changed MAC / WWN addresses" on page 89.
- After replacing the system board in a server running Linux OS, "Updating the NIC configuration file in a Linux environment" on page 86
- "Enabling SVOM boot watchdog functionality" on page 82
- "Enabling BitLocker functionality" on page 88
- Reconfigure your network settings in the operation system according to the original configuration of the replaced controller (expansion card or onboard).

  Configuration of network settings should be performed by the customer.

  For further information, please refer to section "Note on network settings recovery" on page 321.

- If applicable, "After replacing the system board" on page 92.

15 Cables

This chapter provides information on how to connect, disconnect and route cables.

Safety notes

CAUTION!

- Always hold cables by their connectors when disconnecting them. Never pull on the cable to disconnect cables.
- Ensure that none of the cables are scraped, strained or otherwise damaged while replacing system components.
- Immediately replace cables with damaged shielding.
- Always use shielded network cables.

15.1 List of used cables

No	Name	Cable number	Routing	Configuration						
				2	3	4	5	6	7	8
C1	CBL PWR SB 150	T26139-Y3758-V10	from power backplane to system board	o	o	o	o	o	o	o
C2	CBL SMB PWR-BP	T26139-Y4027-V2	from power backplane to system board	o	o	o	o	o	o	o
C4	CBL RX2520M 1 PWR25 GTL	T26139-Y3939-V203	2.5-inch SAS BP(s) to system board	o	o	o	o	o	o	o
C5	CBL PWR 3CO 600	T26139-Y3986-V303	SAS BP(s) to DVD drive	o	o	o	o	o	o	
C6	CBL COMMON FP	T26139-Y4015-V1	Front panel to system board	o	o	o	o	o	o	o

Table 8: List of used cables

No	Name	Cable number	Routing	Configuration						
				2	3	4	5	6	7	8
C7	CBL SAS 2XMINI 110	T26139-Y3963-V111	4x 2.5-inch SAS BP to 12x2.5-inch SAS BP							o
C8	CBL SAS 2XMINI 320	T26139-Y3963-V101	SAS BP to SAS controller				o			
C9	CBL SAS 2XMINI 470	T26139-Y3963-V103	2.5-inch SAS BP to SAS controller			o			2 x o	2 x o
C10	CBL SAS 2XMIN 540	T26139-Y3963-V116	2.5-inch SAS BP to SAS on system board/SAS controller	o	o	o	o	o		
C11	CBL SAS 2XMIN 650	T26139-Y3963-V107	4x2.5-inch SAS BP to SAS controller					o		
C12	CBL LVP	T26139-Y3718-V301	LSD to system board (optional)	o	o	o	o		o	
C14	CBL INT VGA 500	T26139-Y3994-V101	Front VGA to system board (optional)	o	o	o	o	o	o	o
C15	CBL SATA 2XSTR 750	T26139-Y3928-V205	DVD to system board (optional)	o	o	o	o		o	
C17	CBL INT USB 700	T26139-Y3973-V96	tape drive to system board (optional)				o			
C18	CBL MSAS-HDDA	T26139-Y3969-V351	LTO to system board		o			o		
C21	CBL FBU02 170	T26139-Y4032-V3	FBU to controller external HDDs	o	o	o	o	o	o	o

Table 8: List of used cables

No	Name	Cable number	Routing	Configuration						
				2	3	4	5	6	7	8
C22	CBL USB3.0A N 0,8M	T26139-Y4039-A80	USB3.0 cable for RDX3.0 drive				o			

Table 8: List of used cables

15.2 Cabling plans

15.2.1 Configuration 2

4x 2.5-inch HDD model with onboard SAS/SATA controller

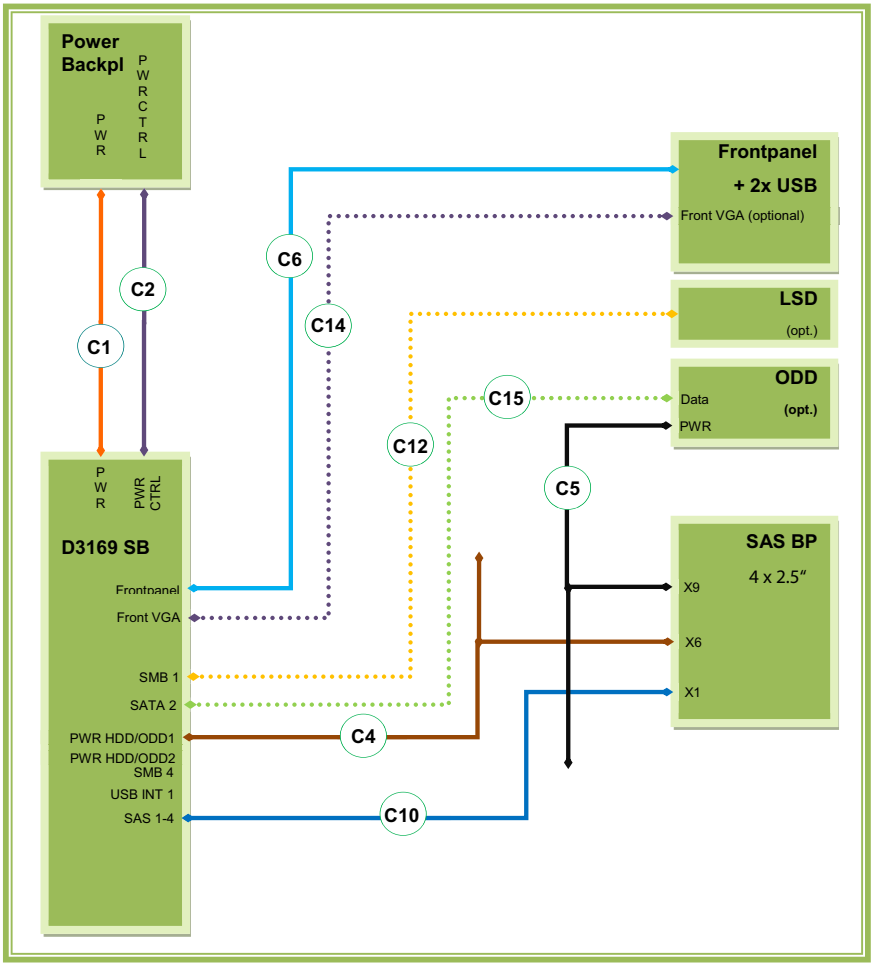


Figure 211: Cabling - 4x 2.5-inch HDD model with SAS onboard connector

4x 2.5-inch HDD model with SAS controller

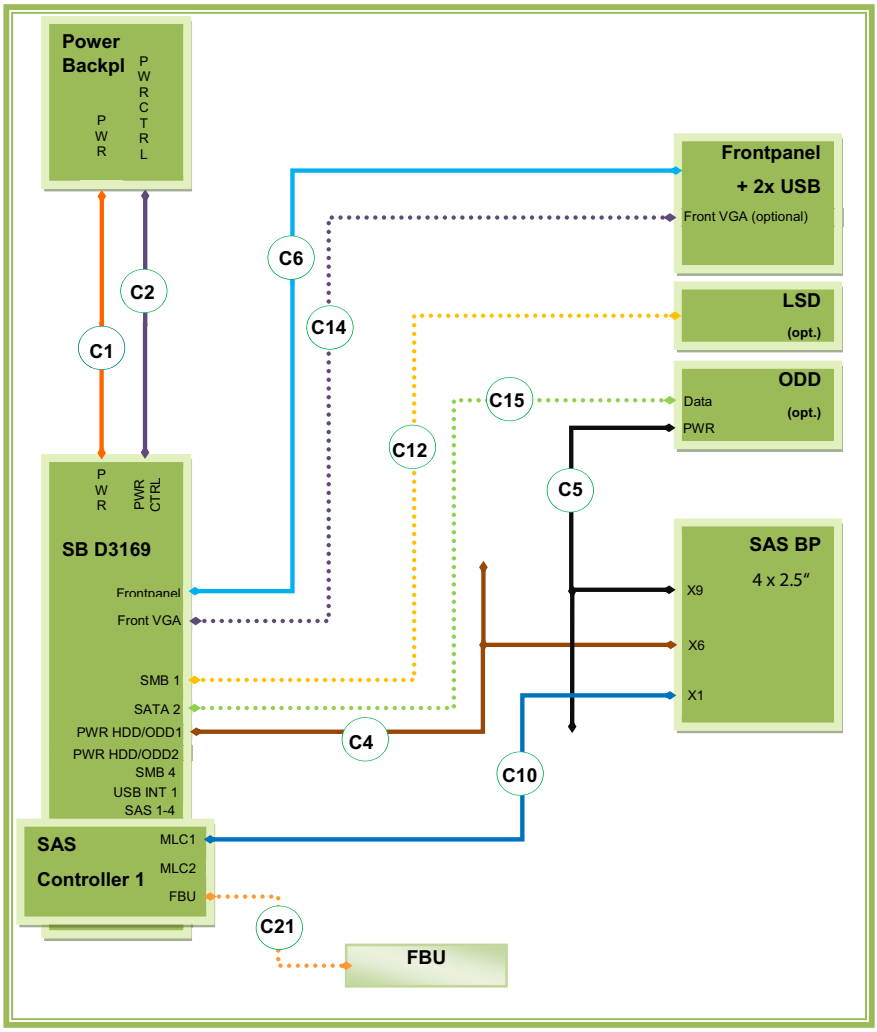


Figure 212: Cabling - 4x 2.5-inch HDD model with SAS controller

15.2.2 Configuration 3

4x 2.5-inch HDD model with LTO drive

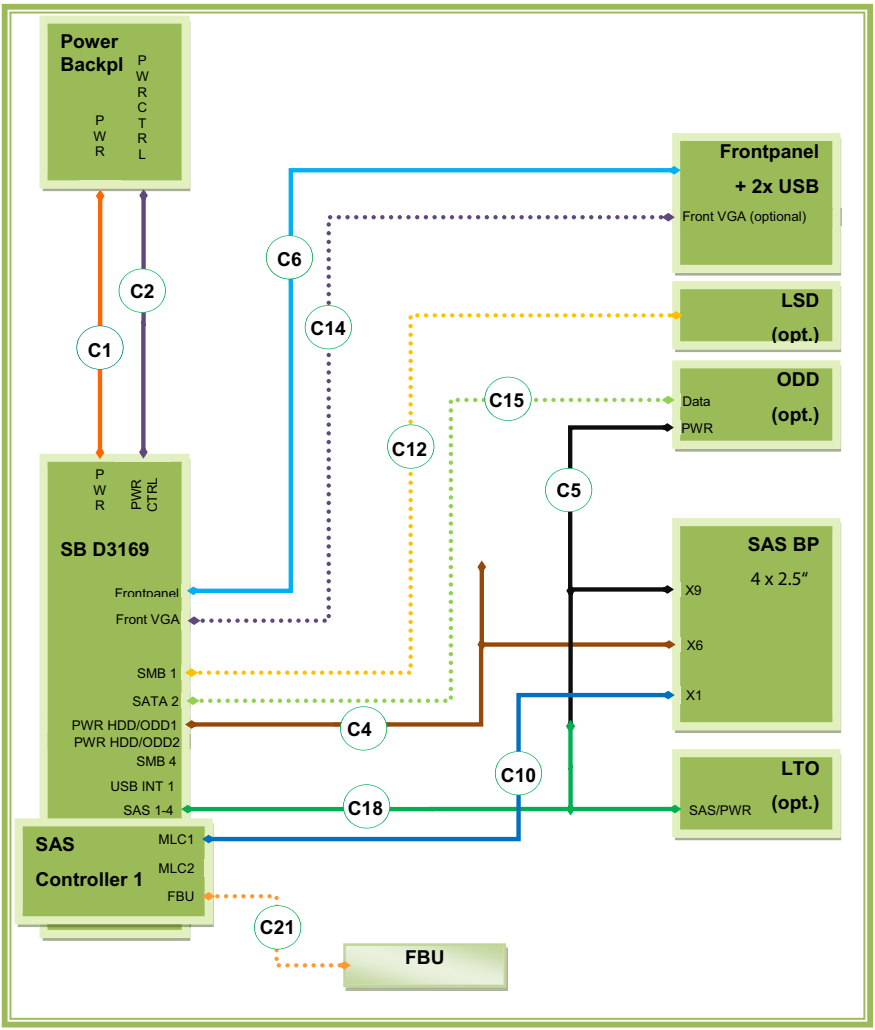


Figure 213: Cabling - 4x 2.5-inch HDD model with LTO drive

15.2.3 Configuration 4

8x 2.5-inch HDD model

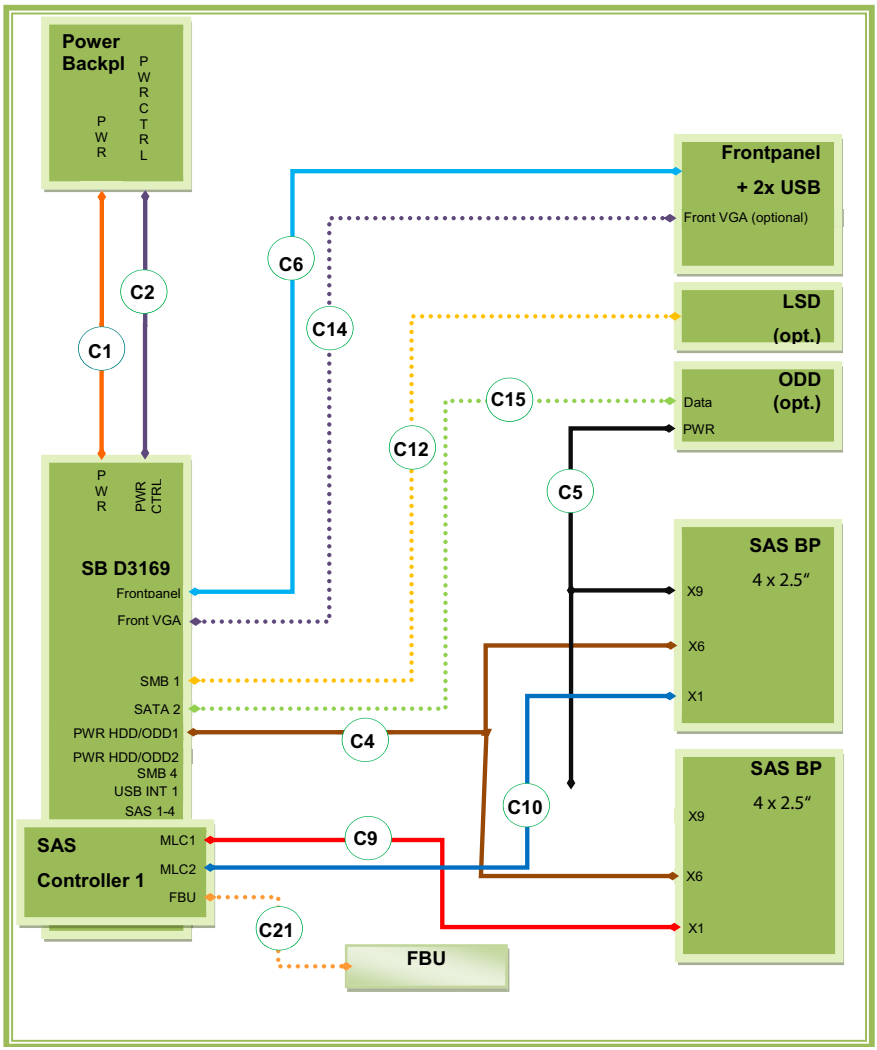


Figure 214: Cabling - 8x 2.5-inch HDD model

15.2.4 Configuration 5

8x 2.5-inch HDD model with optional RDX drive via onboard contr. (USB2.0)

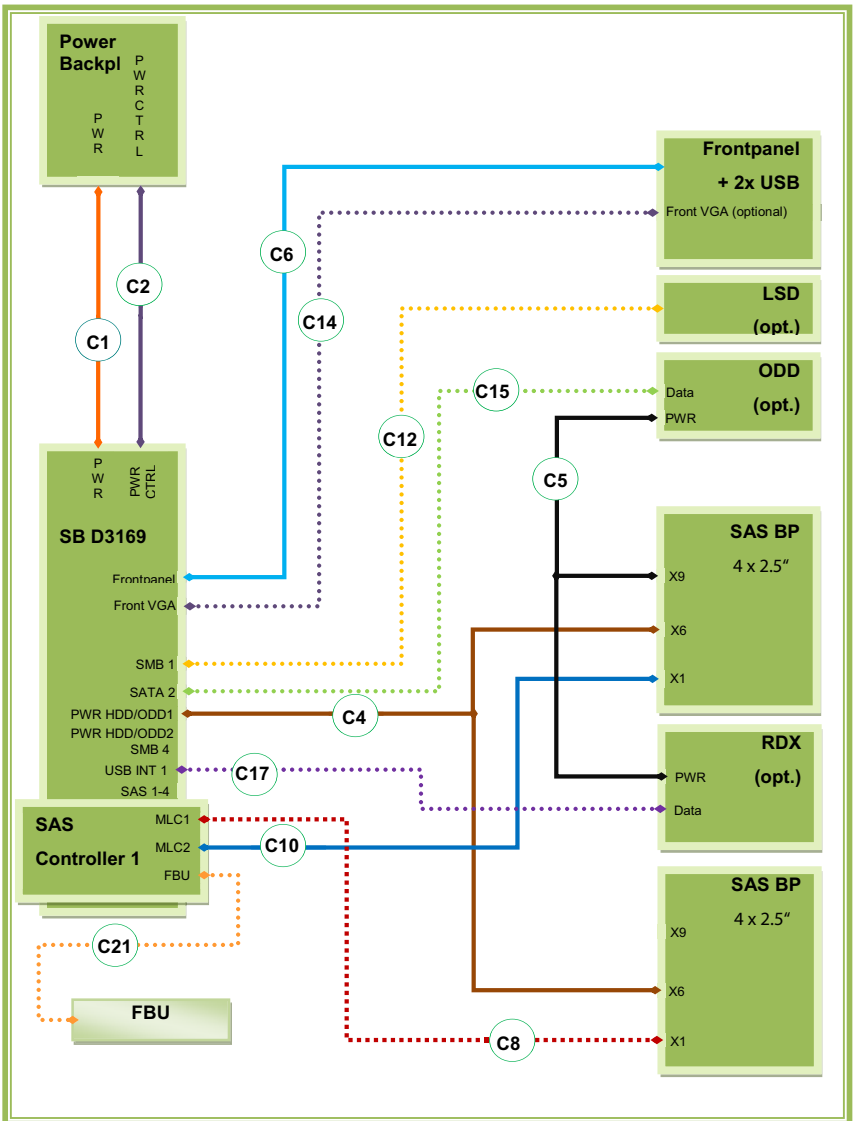


Figure 215: Cabling - 8x 2.5-inch HDD model with RDX drive via onboard connector

8x2.5-inch HDD model with optional RDX drive via interface card (USB 3.0)

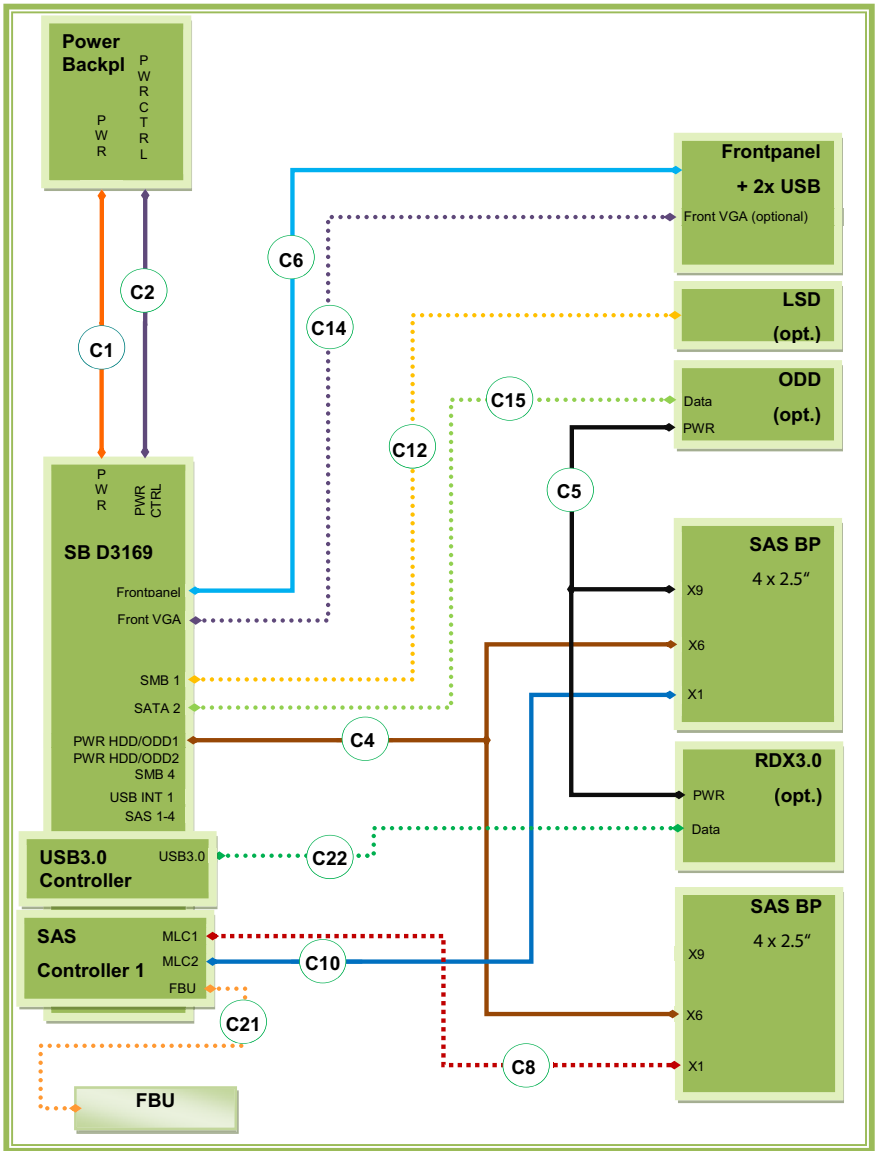


Figure 216: Cabling - 8x 2.5-inch HDD model with RDX drive via USB 3.0 interface card

15.2.5 Configuration 6

8x 2.5-inch HDD model with LTO tape drive

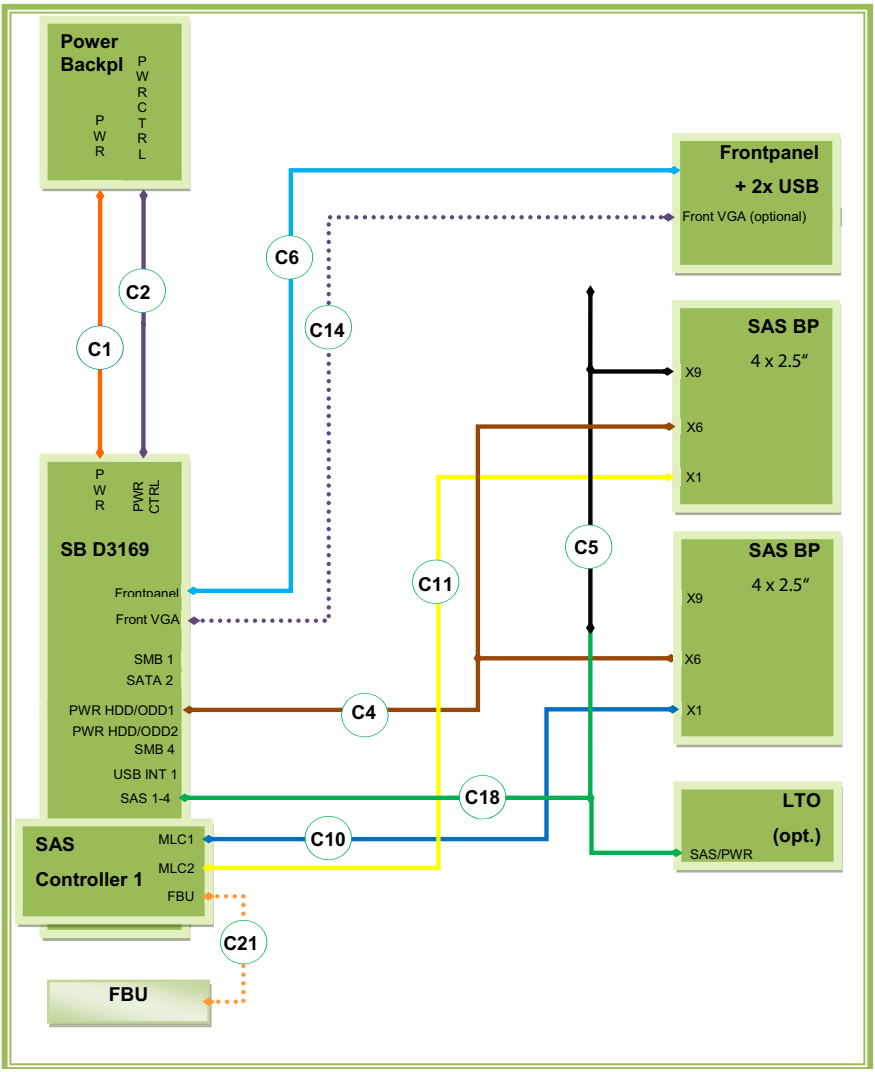


Figure 217: Cabling - 8x 2.5-inch HDD model with LTO4/5/6 tape drive

15.2.6 Configuration 7

12x 2.5-inch HDD model

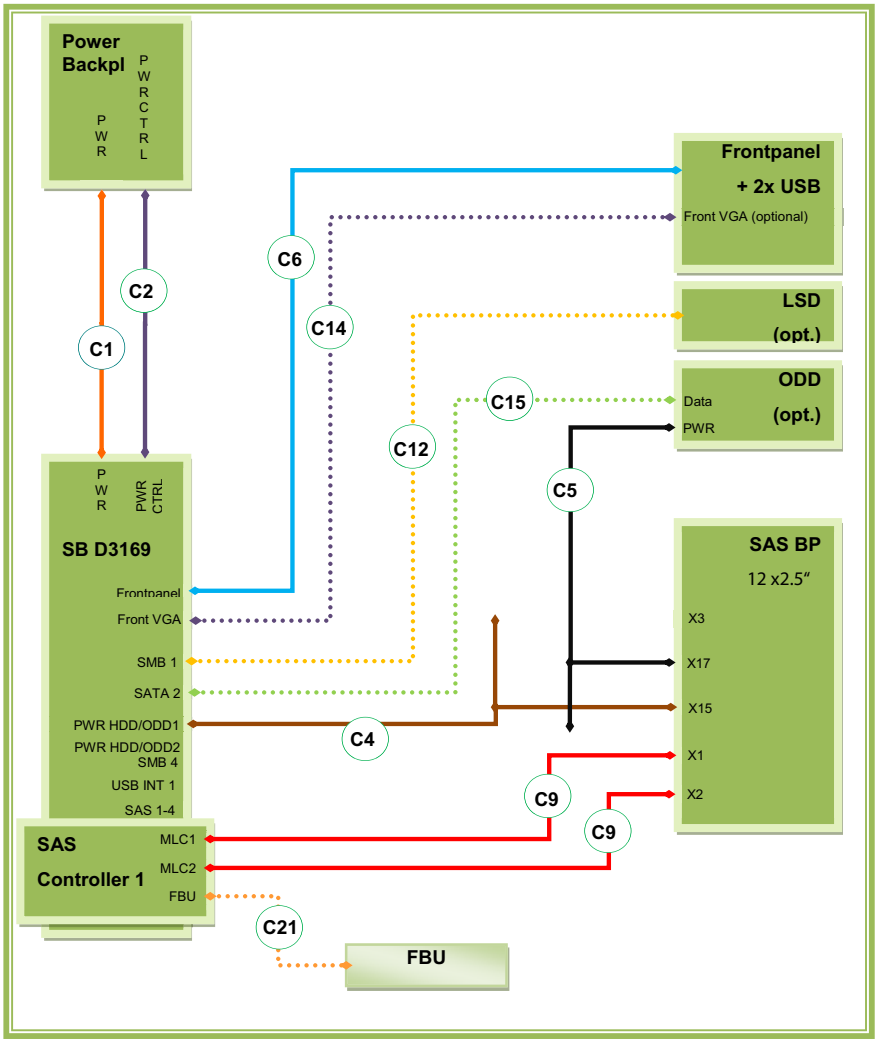


Figure 218: Cabling - 12x2.5-inch HDD model

15.2.7 Configuration 8

16x 2.5-inch HDD model

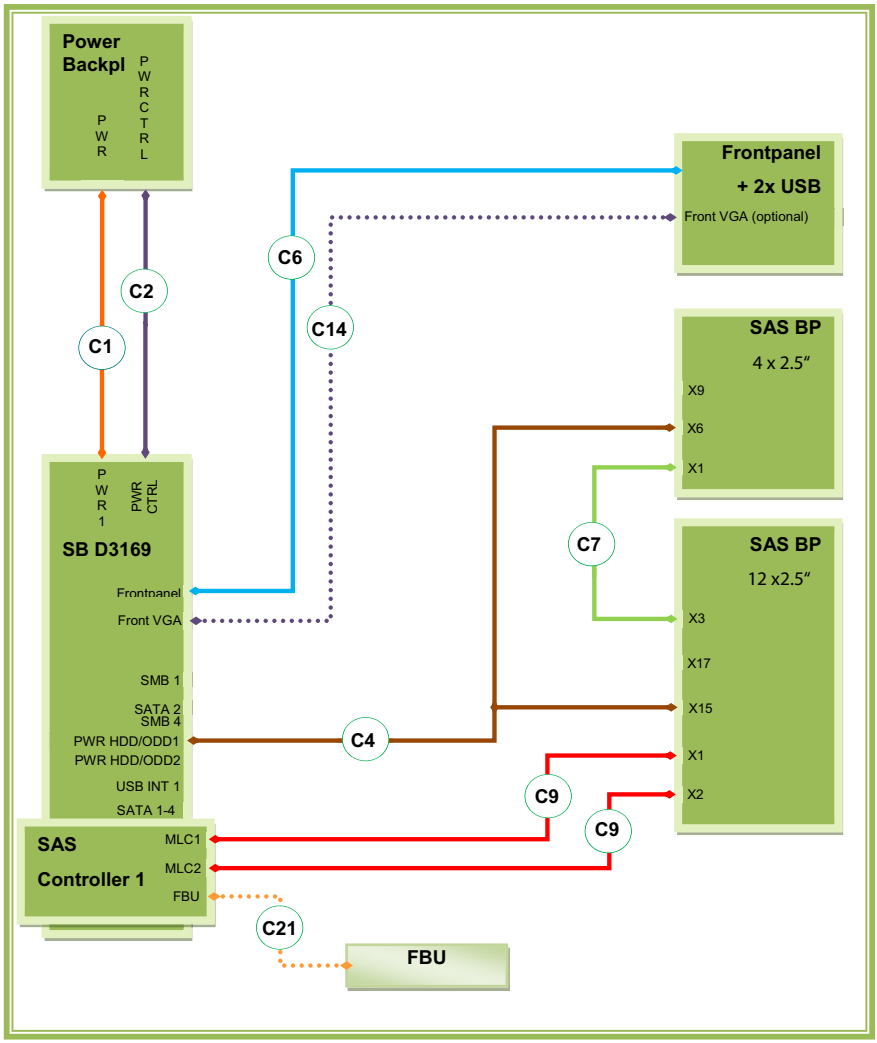


Figure 219: Cabling - 16x 2.5-inch HDD model

16 Appendix

16.1 Mechanical overview

16.1.1 Server front

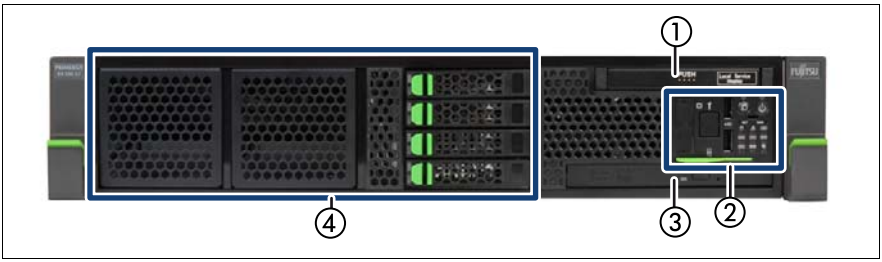


Figure 220: Server front side

Pos.	Component
1	LSD module
2	Front panel module
3	Optical disk drive
4	Space for hard disc drives and backup drives (depending on the configuration)

16.1.2 Server rear

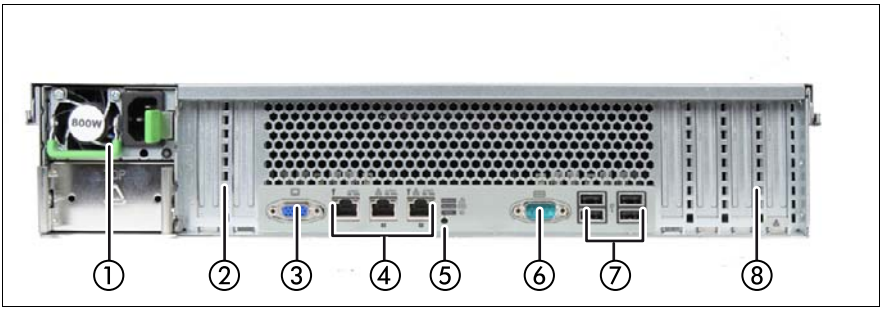


Figure 221: PRIMERGY RX2520 M1 rear

Pos.	Component
1	Power supply unit
2	Optional expansion card
3	VGA video connector
4	LAN connectors
5	CSS / Global Error / ID indicators
6	Serial connector
7	USB connectors 1-4
8	Optional expansion card

16.1.3 Server interior

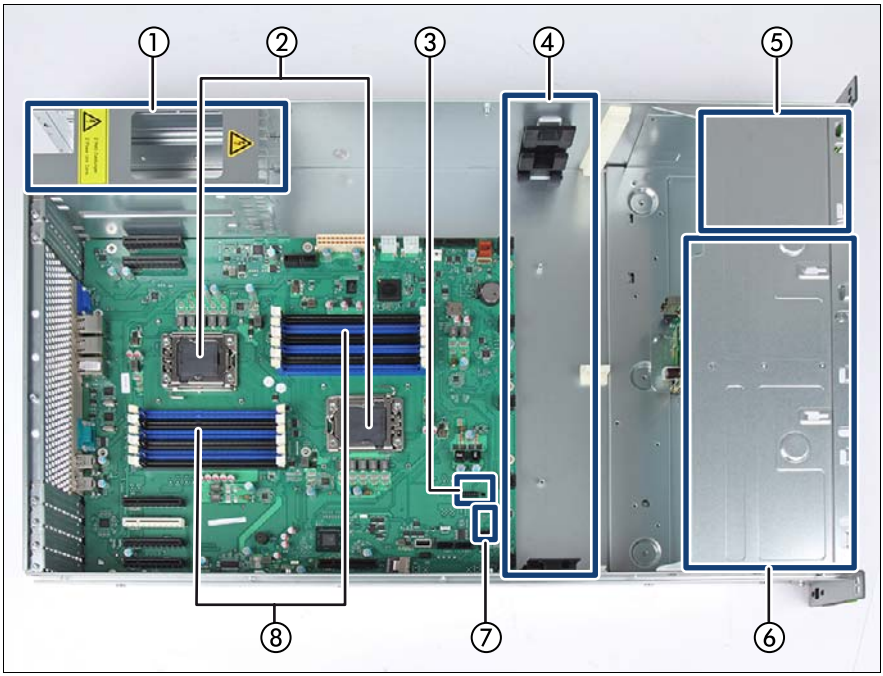


Figure 222: PRIMERGY RX2520 M1 interior (example: 2.5-inch HDD model)

Pos.	Component
1	Power supply units
2	Processor / CPU heat sink
3	TPM
4	Fans
5	Front panel module bay
6	HDD / SSD drive bay
7	UFM
8	Memory slots

16.2 Configuration tables

16.2.1 Hard disk drives / solid state drives mounting order

Please refer to chapter "Hard disk drives / solid state drives" on page 115.

16.2.2 Memory board configuration table

Please refer to chapter "Main memory" on page 195.

16.2.3 Expansion card configuration table

Please refer to chapter "Expansion cards and backup units" on page 149

16.3 Connectors and indicators

16.3.1 Connectors and indicators on the system board

16.3.1.1 Onboard connectors

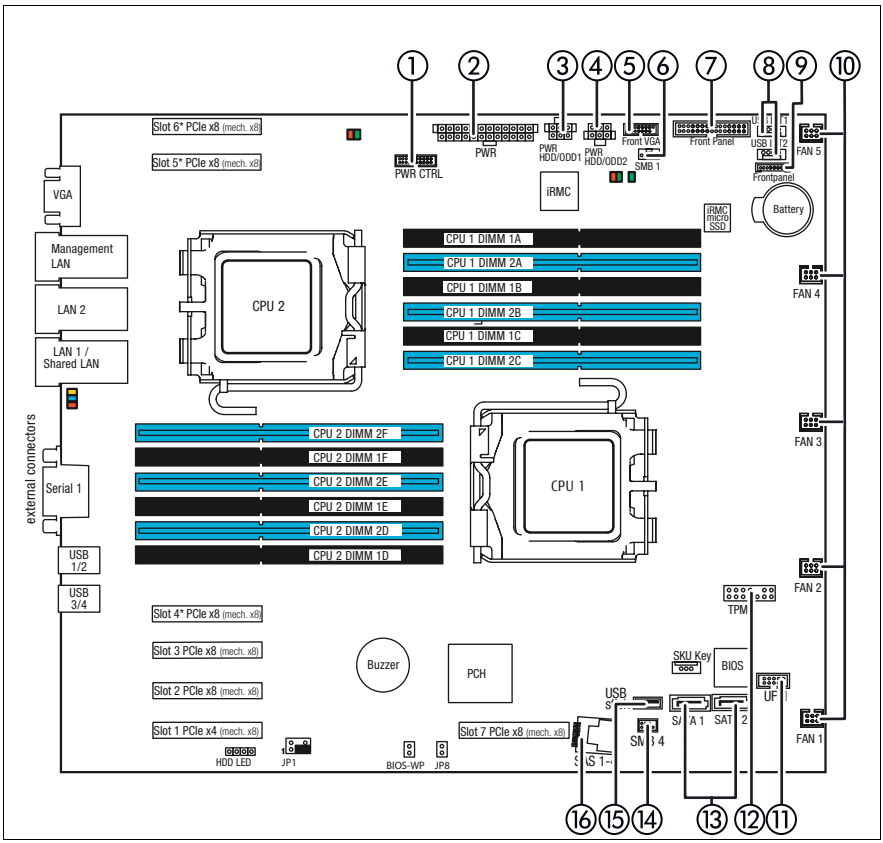


Figure 223: Internal connectors of system board D3169

No.	Print	Description
1	PWR CTRL	Power management connector
2	PWR	ATX power supply connector
3	PWR HDD/ODD 1	left backplane
4	PWR HDD/ODD 2	right backplane
5	Front VGA	Front panel VGA connector
6	SMB 1	LSD module
7	Frontpanel	Front panel connector (2.5-inch version)
8	USB INT 1 / 2	USB 2.0 connectors for USB backup drives
9	Frontpanel	Front panel connector (3.5-inch version)
10	FAN1 - FAN5	FAN connectors
11	UFM	Connector for USB Flash Module (UFM)
12	TPM	Connector for Trusted Platform Module (TPM)
13	SATA 1 / 2	SATA1 / 2 connector
14	SMB 4	
15	SAS 1-4	SATA MLC connector
16	USB stick	

16.3.1.2 Onboard indicators and controls

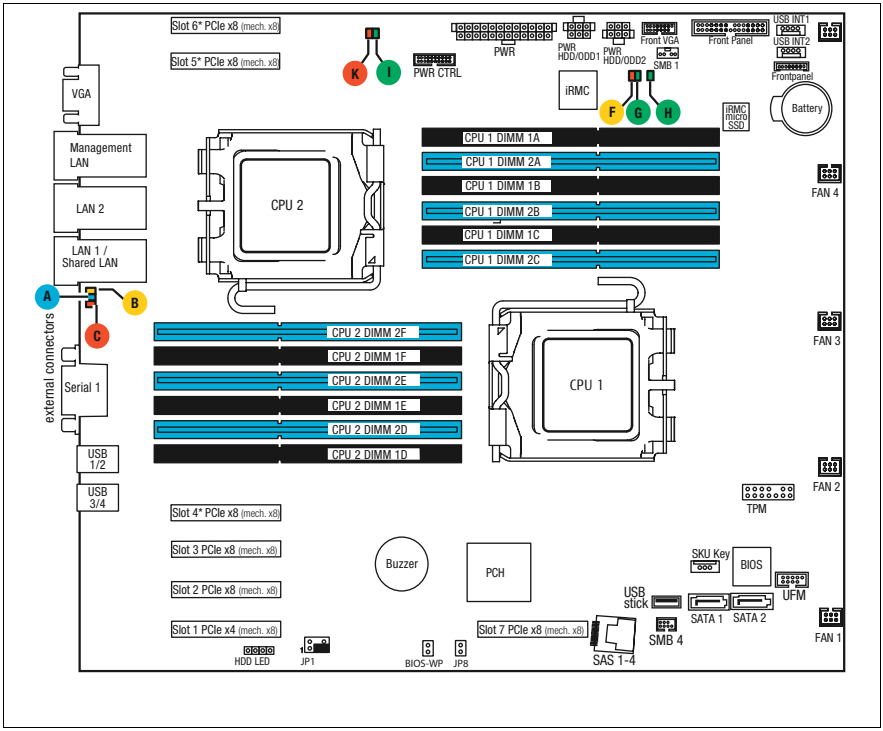


Figure 224: Onboard indicators and Indicate CSS button

Component LEDs

LEDs A, B and C are visible from the outside on the server rear. All other LEDs are only visible if the top cover has been opened.

Indicator		Status	Description
A	Identification	blue on	server has been highlighted using the ID button on the front panel for easy identification
		blue flashing	server has been highlighted using IRMC (AVR) when local VGA off for easy identification

Indicator		Status	Description
B	CSS (Customer Self Service)	off	no critical event (CSS component)
		yellow on	prefailure detected (CSS component)
		yellow flashing	CSS component failure
C	GEL (Global Error LED)	off	no critical event (non CSS component)
		orange on	prefailure detected (non CSS component)
		orange flashing	non CSS component failure Possible reasons: – sensor reports overheating – sensor is defective – CPU error – software reports an error
F	Standby power	yellow on	voltage ok
G	Main power	green on	voltage ok
H	iRMC	green flashing	iRMC S4 ok
I	MBC	green on	power supply OK
K	MBC	orange on	power supply error

16.3.2 Connectors and indicators on the I/O panel

16.3.2.1 I/O panel connectors

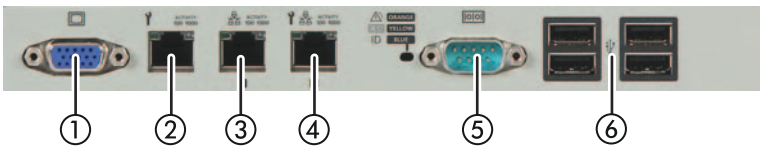


Figure 225: PRIMERGY RX2520 M1 rear

1	Video connector (blue)	4	Shared LAN connector (LAN 1)
2	Management LAN connector	5	Serial connector COM1(turquoise)
3	Standard LAN connector (LAN 2)	6	4 USB connectors (black)

Depending on BIOS settings, the shared LAN connector may also be used as a management LAN connector. For further information, please refer to the corresponding BIOS Setup Utility reference manual.

The serial connector COM1 can be used as default interface or to communicate with the iRMC S4.

The chipset offers two integrated USB 2.0 Rate Matching Hubs (RMHs). that enable lower power requirements and manages the transition of the communication data rate from the high speed of the host controller to the lower speed of USB full speed / low speed devices.

16.3.2.2 I/O panel indicators

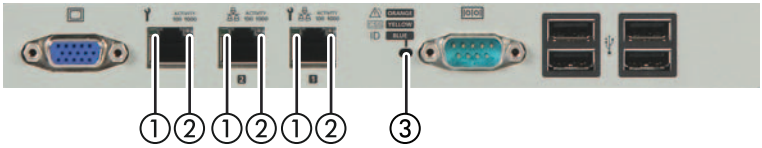


Figure 226: I/O panel indicators

Indicator		Status	Description
1	LAN link/transfer	green on	LAN link
		green flashing	LAN transfer
		OFF	No LAN link
2	LAN speed	OFF	10 Mbit/s
		green on	100 Mbit/s
		yellow on	1000 Mbit/s

Indicator		Status	Description
3	Global error indicator	off	no critical event (non CSS component)
		orange on	prefailure detected (non CSS component)
		orange flashing	non CSS component failure
	CSS indicator	off	no critical event (CSS component)
		yellow on	prefailure detected (CSS component)
		yellow flashing	CSS component failure
	ID indicator	blue on	server has been highlighted using ServerView Operations Manager, iRMC web frontend or the ID button on the front panel for easy identification

Note on the onboard LAN controller

The system board is equipped with a Gigabit Ethernet Controller that supports transfer rates of 10 Mbit/s, 100 Mbit/s and 1 Gbit/s.

The separate management LAN connector is used as a management interface (iRMC S4) and is prepared for operation with the Remote Management. Optionally LAN connector 1 can also be used for iRMC S4 server management.

16.3.3 Connectors and indicators on the front panel

16.3.3.1 Front panel connectors

Figure 227: Front panel controls and indicators

1	Front VGA	2	USB

16.3.3.2 Front panel controls and indicators

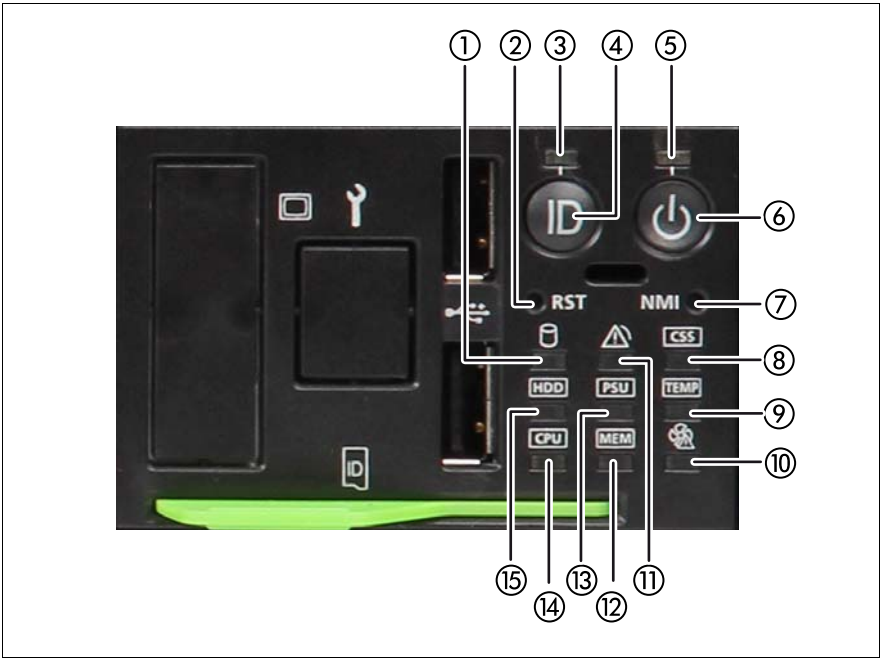


Figure 228: Front side: indicators and controls

1	HDD/SSD activity indicator	9	Temperature error indicator
2	Reset button	10	Fan error indicator
3	ID indicator	11	Global Error indicator
4	ID button	12	Memory error indicator
5	Power-on indicator	13	PSU error indicator
6	On/Off button	14	CPU error indicator
7	NMI button	15	HDD/SSD error indicator
8	CSS indicator		

Local diagnostic indicators

Pos.	Indicator	Status	Description
15	HDD error indicator	orange on	HDD / SSD, SAS / SATA backplane or RAID controller failure detected
13	PSU error indicator	orange on	Hot-plug PSU module failure detected Only available in redundant PSU configurations.
9	Temperature error indicator	orange on	Operating temperature levels above permitted limits
14	CPU error indicator	orange on	CPU prefailure event detected
12	Memory error indicator	orange on	Memory module failure detected
10	Fan error indicator	orange on	System fan prefailure or failure event detected

In addition to local dignostic indicators, CSS or Global Error LEDs indicate, if the defective component is a customer replaceable unit or if a service technician needs to be dispatched to replace the part.

Status indicators

Pos.	Indicator	Status	Description
3	Identification indicator	blue on	server has been highlighted using ServerView Operations Manager, iRMC web frontend or the ID button on the front panel for easy identification
8	CSS indicator	off	no critical event (CSS component)
		yellow on	prefailure detected (CSS component)
		yellow flashing	CSS component failure

Pos.	Indicator	Status	Description
11	Global error indicator	off	no critical event (non CSS component)
		orange on	prefailure detected (non CSS component)
		orange flashing	non CSS component failure
1	HDD / SSD activity indicator	green flashing	data access in progress
5	Power-on indicator	green on	server is switched on and running
		orange on	server is switched off, but mains voltage is present (standby mode) i After connecting the server to the mains it takes about 60 secondes until the server enters the standby mode.

Buttons

Pos.	Button	Function
4	ID button	This button highlights the ID indicator on the front and I/O panels for easy server identification.
2	Reset button	This button is used to reboot the system. It can be pressed using the end of a paper clip. **CAUTION!** Risk of data loss!
7	NMI button	This button is used to troubleshoot software and device driver errors. It can be pressed using the end of a paper clip. **CAUTION!** Use this button only if directed to do so by qualified certified maintenance personnel!
6	On / Off button	This button is used to switch the server on or off. If the system is running an ACPI-compliant operating system, the pressing the On / Off button will performs a graceful shutdown.

16.4 Onboard settings

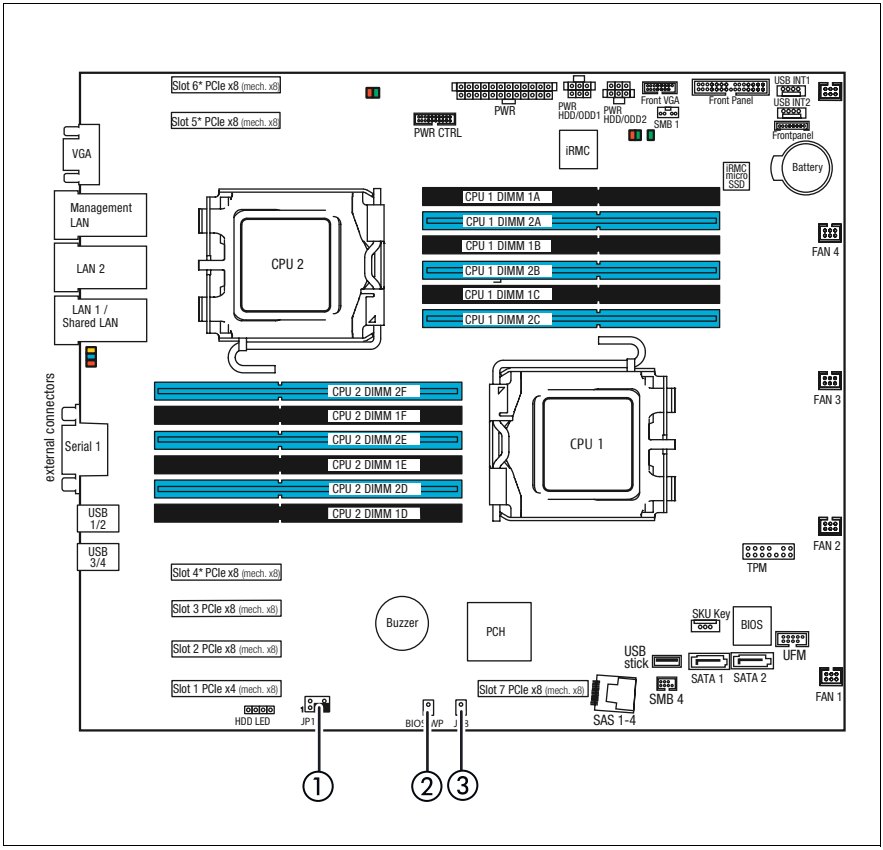
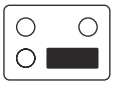
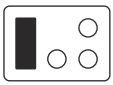
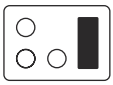


Figure 229: Onboard settings on system board D3169

	Setting		Status	Description
1	JP1	Password Skip/Recovery BIOS		Default: Password delete and Recovery BIOS options disabled
				Password skip enabled This jumper setting will permanently delete the current BIOS password and apply default BIOS settings.
				Recovery BIOS enabled
2	BIOS-WP	Flash Write Protect		Default
				Flash Write Protect enabled
3	JP8	Flash Security Disable		Default
				Flash security disabled

16.5 Minimum startup configuration

Field Replaceable Unit (FRU)

If the server does not start up or other problems occur, it may be necessary to take the system down to its most basic configuration in order to isolate the defective component.

The minimum startup configuration consists of the following components and cables:

Component	Notes
System board	no TPM, UFM or expansion cards installed
CPU with CPU heat sink	
1 memory module	installed in DIMM slot 1A
Front panel module	
Power supply unit	

Table 9: Minimum startup configuration - components

Cable	Notes
Front panel cable	
Power cable	

Table 10: Minimum startup configuration - cables

- "Shutting down the server" on page 49
- "Disconnecting power cords" on page 50
- Take the system down to its minimum startup configuration.
- "Connecting the server to the power source" on page 62
- Connect a keyboard, mouse and display to the server.
- "Switching on the server" on page 64

CAUTION!

Since the fan module is not included in the minimum startup configuration, the server must be shut down immediately after the diagnostic process is complete (POST phase has been passed).

The minimum startup configuration must be used exclusively for diagnostic purposes by maintenance personnel, never in daily operation!